

***MINISTERIO DE ENERGÍA Y MINERÍA DE LA NACIÓN***

***PERMER***

***PRÉSTAMO BANCO MUNDIAL N° 8484-AR***

***“PROVISIÓN DE EQUIPOS DATALOGGER PARA ESCUELAS RURALES Y  
DESARROLLO DE SOFTWARE”***

***LPN: 05/2017***

***PROYECTO DE ENERGIAS RENOVABLES EN MERCADOS  
RURALES***

***PRESTAMO BANCO MUNDIAL N° 8484-AR***

***Fecha de Publicación***

***12 de diciembre de 2017***

## INDICE

---

### A. ASPECTOS GENERALES

- 1.1 Fuente de Recursos
- 1.2 Terminología
- 1.3 Marco legal
- 1.4 Corrupción o Prácticas Fraudulentas
- 1.5 Requisitos para los licitantes

### B. INSTRUCCIONES A LOS LICITANTES

#### 2. Licitación Pública Nacional

- 2.1 Características del procedimiento
- 2.2 Cotización y contratación
- 3. **Ofertas**
  - 3.1 Presentación de las ofertas
  - 3.2 Manifiesto de Garantía de la Oferta
  - 3.3 Documentos que integran la oferta
  - 3.4 Formularios de oferta
  - 3.5 Apertura de las ofertas
  - 3.6 Análisis y evaluación de las ofertas
  - 3.7 Derecho del comprador a aceptar cualquier oferta y a rechazar cualquiera o todas las ofertas
  - 3.8 Adjudicación del Contrato
  - 3.9 Notificación al adjudicatario
  - 3.10 Firma del Contrato
  - 3.11 Garantía de los bienes
  - 3.12 Asociación en Participación o Consorcio
  - 3.13 Ordenes de Cambio y Enmiendas al contrato

### C. PAÍSES ELEGIBLES

### D. CONDICIONES DEL CONTRATO

- 4.1 Plazo de entrega
- 4.2 Contabilidad, inspección y auditoria por el banco de los archivos del proveedor
- 4.3 Inspección y prueba de los bienes
- 4.4 Pago
- 4.5 Intereses por mora en el pago
- 5. Rescisión del contrato
  - 5.1 Rescisión por causa del Proveedor
  - 5.2 Terminación por conveniencia
- 6. Recepción del bien y plazo de garantía
- 7. Prórroga de jurisdicción
- 8. Solución de Controversias

### E. ESPECIFICACIONES TÉCNICAS

Anexo 1: FORMULARIO DE LA OFERTA

Anexo 2: LISTA DE PRECIOS

Anexo 3: SERVICIOS CONEXOS

Anexo 4: MANIFIESTO DE GARANTIA DE LA OFERTA

Anexo 5: LISTA DE BIENES Y PLAN DE ENTREGAS

Anexo 6: AUTORIZACIÓN DEL FABRICANTE

Anexo 7: MODELO DE CONTRATO

Anexo 8: GARANTÍA DE CONTRATO

---

## A. ASPECTOS GENERALES

### 1.1 Fuente de Recursos

1.1.1 La República de Argentina ha recibido del Banco Internacional de Reconstrucción y Fomento (BIRF) un préstamo para financiar parcialmente el costo del Proyecto de Energías Renovables en Mercados Rurales (PERMER) dependiente del Ministerio de Energía y Minería de La Nación, BIRF 8484-AR. Podrán participar en la licitación todos los licitantes de los países que reúnan los requisitos de elegibilidad que se estipulan en las *Normas de Adquisiciones del BIRF y la Sección C*.

### 1.2 Terminología

1.2.1 Las expresiones que aquí se definen se aplican al presente documento y a sus formularios y planillas adjuntas:

Receptora - Prestatario: es la República de Argentina.

BIRF o Banco: es el Banco Internacional de Reconstrucción y Fomento (BIRF).

Préstamo: es el Convenio de Préstamo 8484 - AR celebrado entre el BIRF y el Prestatario.

Proyecto: es el Proyecto de Energías Renovables en Mercados Rurales.

**Comprador:** La Subsecretaría de Energías Renovables a través del Proyecto de Energías Renovables en Mercados Rurales (PERMER) dependiente del Ministerio de Energía y Minería de La Nación es la persona jurídica del derecho público, que encarga la adquisición de los bienes y figura designada como tal en las Bases y Condiciones que integran la documentación de esta Licitación Pública Nacional.

**Proveedor:** es la persona de existencia ideal o visible que ha formalizado el Contrato y se encuentra obligada al suministro de los bienes, en los términos previstos.

**Días:** son días calendario.

**Meses:** son meses calendario.

### 1.3 Marco legal

1.3.1 El Proyecto está obligado durante la adquisición a regirse por las normas del Convenio de Préstamo, las Normas de Contrataciones con préstamos del BIRF y Créditos AIF, de mayo 2004 versión revisada en enero de 2011, y las estipulaciones del presente documento. Cuando exista vacío normativo o deba resolverse sobre aspectos no reglamentados en este Documento de Licitación, se aplicarán supletoriamente las normas que de acuerdo a derecho correspondan a la jurisdicción del Contratante y a la personería de éste, siempre que no se opongan a lo establecido en: i) el Convenio de Préstamo y ii) las Normas de Contrataciones con préstamos del BIRF y Créditos AIF, de mayo 2004 versión revisada en enero de 2011.

1.3.2 En todos los casos y cualquiera sea la personería del Contratante, se entenderá que el Contrato que se celebre con el adjudicatario de la Licitación, es un Contrato de provisión de bienes regido por la ley de la República Argentina.

### 1.4 Corrupción o Prácticas Fraudulentas

1.4.1 El Banco exige que todos los Prestatarios (incluidos los beneficiarios de préstamos concedidos por el Banco), así como los Licitantes, proveedores, contratistas y sus agentes (hayan sido declarados o no), el personal, los subcontratistas, subconsultores, proveedores de servicios o proveedores de insumos, y cualquier otro personal asociado, observen las más elevadas normas éticas

---

durante el proceso de contrataciones y la ejecución de los contratos financiados por el Banco<sup>1</sup>. Para dar cumplimiento a esta política, el Banco:

- (a) define, para efectos de esta disposición, las siguientes expresiones:
- (i) “práctica corrupta” significa el ofrecimiento, suministro, aceptación o solicitud, directa o indirectamente, de cualquier cosa de valor con el fin de influir impropriamente en la actuación de otra persona<sup>2</sup>;
  - (ii) “práctica fraudulenta” significa cualquier actuación u omisión, incluyendo una tergiversación de los hechos que, astuta o descuidadamente, desorienta o intenta desorientar a otra persona con el fin de obtener un beneficio financiero o de otra índole, o para evitar una obligación<sup>3</sup>;
  - (iii) “práctica de colusión” significa un arreglo de dos o más personas<sup>4</sup> diseñado para lograr un propósito impropio, incluyendo influenciar impropriamente las acciones de otra persona;
  - (iv) “práctica coercitiva” significa el daño o amenazas para dañar, directa o indirectamente, a cualquiera persona, o las propiedades de una persona, para influenciar impropriamente sus actuaciones<sup>5</sup>.
  - (v) “práctica de obstrucción” significa
    - (aa) la destrucción, falsificación, alteración o escondimiento deliberados de evidencia material relativa a una investigación o brindar testimonios falsos a los investigadores para impedir materialmente una investigación por parte del Banco, de alegaciones de prácticas corruptas, fraudulentas, coercitivas o de colusión; y/o la amenaza, persecución o intimidación de cualquier persona para evitar que pueda revelar lo que conoce sobre asuntos relevantes a la investigación o lleve a cabo la investigación, o
    - (bb) las actuaciones dirigidas a impedir materialmente el ejercicio de los derechos del Banco a inspeccionar y auditar de conformidad con la Subcláusula (e), mencionada más abajo.
- (b) rechazará toda propuesta de adjudicación si determina que el licitante seleccionado para dicha adjudicación o su personal, sus agentes y subconsultores, subcontratistas, proveedores o sus empleados hayan participado, directa o indirectamente, en prácticas corruptas, fraudulentas, de colusión, coercitivas o de obstrucción para competir por el Contrato de que se trate;
- (c) declarará la adquisición viciada y anulará la porción del préstamo asignada a un contrato si en cualquier momento determina que los representantes del Prestatario o de un beneficiario de alguna parte de los fondos del préstamo han participado en prácticas corruptas, fraudulentas, de colusión, coercitivas o de obstrucción durante el proceso de adquisición o la implementación de dicho contrato, sin que el Prestatario haya adoptado medidas oportunas y apropiadas que el Banco considere satisfactorias para corregir la situación, dirigidas a dichas prácticas cuando éstas ocurran, incluyendo no haber informado al Banco oportunamente el haberse conocido esas prácticas;

---

<sup>1</sup> En este contexto, cualquier acción para influenciar el proceso de contratación o de ejecución de un contrato, para adquirir una ventaja ilegítima, es impropia.

<sup>2</sup> “Persona” se refiere a un funcionario público que actúa con relación al proceso de contratación o la ejecución del contrato. En este contexto, “funcionario público” incluye a personal del Banco Mundial y a empleados de otras organizaciones que toman o revisan decisiones relativas a los contratos.

<sup>3</sup> “Persona” significa un funcionario público; los términos “beneficio” y “obligación” se refieren al proceso de contratación o a la ejecución del contrato; y el término “actuación u omisión” debe estar dirigida a influenciar el proceso de contratación o la ejecución de un contrato.

<sup>4</sup> “Personas” se refiere a los participantes en el proceso de contratación (incluyendo a funcionarios públicos) que intentan, por sí mismos o por medio de otra persona o entidad no participante del proceso, establecer precios de oferta a niveles artificiales y no competitivos.

<sup>5</sup> “Persona” se refiere a un participante en el proceso de contratación o en la ejecución de un contrato. —

(d) sancionará a una firma o persona, en cualquier momento, de conformidad con el régimen de sanciones del Banco, incluyendo declarar dicha firma o persona inelegible públicamente, en forma indefinida o durante un período determinado para: i) que se le adjudique un contrato financiado por el Banco y ii) que se le nomine subcontratista, consultor, fabricante o proveedor de productos o servicios de una firma que de lo contrario sería elegible para que se le adjudicara un contrato financiado por el Banco.

(e) requerirá que, en los contratos financiados con un préstamo del Banco, se incluya una cláusula que exija que los Licitantes, proveedores y contratistas y sus subcontratistas, sus agentes, personal, consultores, proveedores de bienes o servicios deben permitir al Banco revisar todas las cuentas, archivos y otros documentos relacionados con la presentación de las ofertas y el cumplimiento del contrato y someterlos a una verificación por auditores designados por el Banco.

1.4.2 Además, los Licitantes deberán tener presente las provisiones establecidas en la Subcláusula 5.1.1 (b) de las Condiciones del Contrato.

## **1.5 Requisitos para los Licitantes**

1.5.1 Un Licitante, y todas las partes que constituyen el Licitante, pueden tener la nacionalidad de cualquier país, de conformidad con las condiciones estipuladas en la Sección C, Países Elegibles. Se considerará que un Licitante tiene la nacionalidad de un país si es ciudadano o está constituido, incorporado o registrado y opera de conformidad con las disposiciones legales de ese país. Este criterio también aplicará para determinar la nacionalidad de los subcontratistas o proveedores propuestos para la ejecución de cualquier parte del Contrato incluso los Servicios Conexos.

1.5.2 Un Licitante no deberá tener conflicto de interés. Los Licitantes que sean considerados que tienen conflicto de interés serán descalificados. Se considerará que los Licitantes tienen conflicto de interés con una o más partes en este proceso de licitación si ellos:

(a) están o han estado asociados, directa o indirectamente, con una firma o con cualquiera de sus afiliados, que ha sido contratada por el Comprador para la prestación de servicios de consultoría para la preparación del diseño, las especificaciones técnicas y otros documentos que se utilizarán en la licitación para la adquisición de los bienes objeto de estos Documentos de Licitación; o

(b) presentan más de una oferta en este proceso licitatorio.

1.5.3 Una firma que haya sido inhabilitada por el Banco de acuerdo a lo establecido en la Subcláusula 1.4.1 (d) de la Sección A, o de acuerdo con las Normas para la Prevención y Lucha contra el Fraude y la Corrupción en proyectos financiados por préstamos del BIRF y donaciones de la (AIF) estará inhabilitada para la adjudicación de contratos financiados por el Banco o recibir cualquier beneficio de un contrato financiado por el Banco, financiero o de otra índole, durante el periodo determinado por el Banco. La lista de firmas inhabilitadas se encuentra disponible en la dirección electrónica que se indica a continuación: <http://www.worldbank.org/debarr>.

1.5.4 Las empresas estatales del país Prestatario serán elegibles solamente si pueden demostrar que (i) tienen autonomía legal y financiera; (ii) operan conforme a las leyes comerciales; y (iii) no dependen de ninguna agencia del Comprador.

1.5.5 Los Licitantes deberán proporcionar al Comprador evidencia satisfactoria de su continua elegibilidad, cuando el Comprador razonablemente la solicite.

---

## B. INSTRUCCIONES A LOS LICITANTES

### 2. Licitación Pública Nacional

#### 2.1 Características del procedimiento

2.1.1 Todo Licitante potencial que requiera alguna aclaración sobre los Documentos de Licitación deberá comunicarse con el Comprador por escrito a la dirección del Comprador: mediante correo electrónico a: **compraspermer@minem.gob.ar**. El Comprador responderá por escrito a todas las solicitudes de aclaración, siempre que dichas solicitudes sean recibidas al menos catorce (14) días antes de la fecha límite para la presentación de ofertas. El Contratante responderá en forma de Circular las solicitudes de aclaración y se publicará en los siguientes sitios: portal del PERMER: [www.permer.minem.gob.ar](http://www.permer.minem.gob.ar) siendo responsabilidad exclusiva de los licitantes la consulta de las páginas para acceder a todas las circulares, no pudiendo reclamar basados en su desconocimiento.

Si como resultado de las aclaraciones el Comprador considera necesario enmendar los Documentos de Licitación, deberá hacerlo siguiendo el procedimiento indicado en la Subcláusula 2.1.2 y en la Subcláusula 3.1.3.

2.1.2 El Comprador podrá, en cualquier momento antes del vencimiento del plazo para presentación de ofertas, enmendar los Documentos de Licitación mediante la emisión de una enmienda. Toda enmienda emitida formará parte integral de los Documentos de Licitación y deberá ser comunicada por escrito a todos los que hayan obtenido los documentos de Licitación directamente del Comprador.

#### 2.2 Cotización y contratación

2.2.1 El licitante cotizará un precio único por el que se compromete a proveer los bienes solicitados. Los precios cotizados para cada Lote deberán corresponder al 100% de los artículos listados para cada Lote. La cotización y contratación se deberá hacer en pesos argentinos. Si se solicita además del bien, otras provisiones o servicios conexos, deberán ser cotizadas de forma separada del precio del bien, excepto que se solicite su inclusión en un monto único. En el Formulario de la Oferta deberá consignarse el precio total de la oferta.

2.2.2 Los precios deberán registrarse de la siguiente manera:

(a) El precio de los bienes cotizados debe ser DDP (que incluye precio neto del artículo, impuestos, derechos de importación, transporte hasta destino final indicado en el Anexo 5, flete y seguro);

(b) Para los Servicios Conexos, cuando dichos Servicios Conexos sean especificados en la Lista de Bienes y Servicios:

(i) el precio de cada artículo que comprende los Servicios Conexos (inclusive cualquier impuesto aplicable).

2.2.3 A los fines de esta Subcláusula la edición de Incoterms es Incoterms 2010.

2.2.4 Los Licitantes podrán presentar oferta por uno o más lotes.

Los precios cotizados para cada lote deberán corresponder al ciento por ciento (100%) de las cantidades indicadas para cada lote.

Los Licitantes podrán ofrecer descuentos por la adjudicación de más de un lote, para lo cual deberán indicar en el Formulario de la oferta la metodología aplicable.

---

### 3. Ofertas

#### 3.1 Presentación de las ofertas

- 3.1.1 La presentación de las ofertas se efectuará en original y 2 copias, en un sobre único cerrado, en el lugar, día y hora, especificados en el llamado a licitación, con la siguiente leyenda en su exterior:

**Licitación Pública Nacional N°05/2017 “Código STEP AR-SE-31237-GO-RFB”**

**Nombre del Contratante:** SUBSECRETARÍA DE ENERGÍAS RENOVABLES-PERMER

**Denominación de la adquisición:** “Provisión de 500 equipos datalogger para escuelas rurales y desarrollo de software “

**Lugar de Apertura:** Av. Paseo colón 171, Piso 9º oficina 902. De la Ciudad de Buenos Aires (CABA) Código Postal C1053ACB

**Fecha y hora de apertura:** 18 de enero de 2017 a las 12:30 horas.

**Nombre y dirección del Licitante:** Av. Eduardo Madero 942. Piso 15 C1105ACW.

- 3.1.2 Las ofertas deberán ser recibidas por el Comprador en la dirección indicada arriba y en el Llamado a Licitación, y tendrán una **validez de noventa (90) días** a partir de la fecha de su apertura y los documentos que las integran deberán presentarse firmados por el Licitante, en todas sus fojas.
- 3.1.3 En circunstancias excepcionales y antes de que expire el período de validez de la oferta, el Comprador podrá solicitarle a los Licitantes que extiendan el período de la validez de sus ofertas. Las solicitudes y las respuestas deberán hacerse por escrito. Al Licitante que acepte la solicitud de prórroga no se le pedirá ni permitirá modificar su oferta.
- 3.1.4 En el caso de contratos con precio fijo, si la adjudicación se retrasase por un período mayor a cincuenta y seis (56) días a partir del vencimiento del plazo inicial de validez de la oferta, el precio del Contrato será ajustado según lo especificado en la solicitud de prórroga. La evaluación de la oferta deberá basarse en el precio cotizado sin tomar en cuenta el ajuste mencionado.

#### 3.2 Manifiesto de Garantía de la Oferta

- 3.2.1 Todas las ofertas deberán incluir un Manifiesto de Garantía de la Oferta, usando el modelo indicado en el Anexo 4 de estos documentos.
- 3.2.2 El Manifiesto de Garantía de la Oferta de una Asociación en Participación o Consorcio deberá ser emitido en nombre de la Asociación en Participación o Consorcio que presenta la oferta. Si dicha Asociación o Consorcio no ha sido legalmente constituido en el momento de presentar la oferta, el Manifiesto de Seriedad de la Oferta deberá ser emitido en nombre de todos los futuros socios de la Asociación o Consorcio y firmada por cada miembro.

#### 3.3 Documentos que integran la oferta

- 3.3.1 La oferta deberá incluir los siguientes documentos:
- (a) Formulario de la Oferta (Anexo 1);
  - (b) Lista de cantidades y precios de cada artículo (Anexo 2)
  - (c) Formulario de Servicios Conexos –en caso de corresponder- (Anexo 3);
  - (d) Especificaciones técnicas de los bienes ofertados, pudiendo incluirse adicionalmente Folletos generales de los bienes;
  - (e) Documentación autenticada relativa a la constitución o condición jurídica del licitante; un poder (escritura pública) en que se otorguen facultades al firmante de la oferta para comprometer al licitante;
  - (f) Manifiesto de Garantía de la Oferta (Anexo 4).
  - (g) Copia de los estados financieros de los últimos dos ejercicios cerrados, certificado por el Consejo Profesional respectivo y auditado por profesional independiente. Si

el último estado financiero a presentar tuviera una antigüedad igual o mayor a un año al de la fecha de presentación de ofertas, el Licitante deberá acompañar la facturación correspondiente desde la fecha de cierre del último balance presentado hasta la actualidad, certificada por Contador Público Nacional y legalizada su firma por el Consejo Profesional respectivo;

### **3.4 Formularios de oferta**

3.4.1 El Licitante llenará el formulario de oferta incluido como Anexo 1, la lista de precios que se incluye en el Anexo 2 de estos documentos de licitación y el formulario de servicios conexos, si corresponde, indicado en el Anexo 3, e indicará la cantidad, los precios y el país de origen de los bienes que suministrará, y una breve descripción de los mismos. Asimismo, el Licitante deberá completar el Manifiesto de Garantía de la Oferta, indicado en el Anexo 4.

3.4.2 El Licitante que no fabrica o produce los bienes que propone proveer deberá presentar una Autorización del Fabricante mediante el formulario incluido en el Anexo 6 para demostrar que ha sido debidamente autorizado por el fabricante o productor de los Bienes para suministrarlos en el país del Comprador.

### **3.5 Apertura de las ofertas**

3.5.1 En el lugar, fecha y hora especificado en la Invitación se abrirán los sobres con las ofertas, en presencia de los responsables de la Comisión de Apertura que la Unidad Ejecutora del Programa designe y de los representantes de las empresas que deseen asistir, elaborándose un acta a tal efecto, en la que deberá constar:

- (a) Nombre de los responsables designados por la Unidad Ejecutora del Programa.
- (b) Nombre de los representantes de los licitantes que se encuentren presentes.
- (c) Monto de las ofertas.
- (d) Presentación del Manifiesto de Garantía de la Oferta.
- (e) Cualquier otra observación que se formule.
- (f) Toda otra circunstancia relacionada con el acto, que el funcionario responsable estime oportuno consignar.

Dicha acta deberá estar firmada por los responsables que se consignan en el literal "a" del presente artículo y por los representantes de los licitantes que se encuentren presentes conforme el literal "b".

3.5.2 Las ofertas presentadas con posterioridad a la fecha y hora límites indicadas en el aviso de licitación, serán devueltas sin abrir.

3.5.3 Un Licitante podrá retirar, sustituir o modificar su oferta después de presentada mediante el envío de una comunicación por escrito, de conformidad con la Subcláusula 3.1.1 debidamente firmada por un representante autorizado, y deberá incluir una copia de dicha autorización (poder judicial). La sustitución o modificación correspondiente de la oferta deberá acompañar dicha comunicación por escrito. Todas las comunicaciones deberán ser recibidas por el Comprador antes del plazo límite establecido para la presentación de las ofertas, de conformidad con la Subcláusula 3.1.1. Los sobres deberán estar claramente marcados "RETIRO", "SUSTITUCIÓN" o "MODIFICACIÓN".

Las ofertas cuyo retiro fue solicitado de conformidad con la presente Subcláusula serán devueltas sin abrir a los Licitantes remitentes.

Ninguna oferta podrá ser retirada, sustituida o modificada durante el intervalo comprendido entre la fecha límite para presentar ofertas y la expiración del período de validez de las ofertas indicado por el Licitante en el Formulario de Oferta, o cualquier extensión si la hubiese.

---



### 3.6 Análisis y evaluación de las ofertas

3.6.1 La información relativa al examen, aclaración, evaluación y comparación de las ofertas y las recomendaciones para la adjudicación de un contrato no podrán ser reveladas a los licitantes ni a ninguna otra persona que no participe oficialmente en dicho proceso hasta que se haya anunciado el nombre del Adjudicatario. Todo intento de un Licitante de influir en la tramitación de las ofertas o en la decisión sobre la adjudicación por parte del Contratante puede dar lugar al rechazo de la oferta de ese Licitante.

3.6.2 El Comprador examinará las ofertas para determinar si están completas, si contienen errores de cálculo, si se han presentado las garantías requeridas y si los documentos han sido debidamente firmados. En caso de errores aritméticos procederá a corregirlos de la siguiente manera:

- (a) si hay una discrepancia entre un precio unitario y el precio total obtenido al multiplicar ese precio unitario por las cantidades correspondientes, prevalecerá el precio unitario y el precio total será corregido a menos que el Comprador considere que hay un error obvio en la colocación del punto decimal, caso en el cual el total cotizado prevalecerá y el precio unitario se corregirá;
- (b) si hay un error en un total que corresponde a la suma o resta de subtotales, los subtotales prevalecerán y se corregirá el total; y
- (c) si hay una discrepancia entre palabras y cifras, prevalecerá el monto expresado en palabras a menos que la cantidad expresada en palabras corresponda a un error aritmético, en cuyo caso prevalecerán las cantidades en cifras de conformidad con los párrafos (a) y (b) mencionados.

Si el Licitante que presentó la oferta evaluada más baja no acepta la corrección de los errores, su oferta podrá ser rechazada y se podrá ejecutar el Manifiesto de Garantía de la Oferta.

3.6.3 El Comprador examinará todas las ofertas para confirmar que todos los documentos y documentación técnica solicitada en la Subcláusula 3.3 de la Sección B han sido suministrados y para determinar si cada documento entregado está completo.

3.6.4 El Comprador confirmará que los siguientes documentos e información han sido proporcionados con la oferta. Si cualquiera de estos documentos o información faltaran, la oferta será rechazada.

- (a) Formulario de Oferta firmado, de conformidad con el formulario del Anexo 1;
- (b) Lista de Precios firmada, de conformidad con el formulario del Anexo 2;
- (c) Formulario de Servicios Conexos firmado, si corresponde, de conformidad con el formulario del Anexo 3;
- (d) Manifiesto de Garantía de la Oferta firmado, de conformidad con el formulario del Anexo 4.

Las ofertas que no se ajusten al período de validez indicado en la Subcláusula 3.1.2 de la Sección B, podrán ser rechazadas.

3.6.5 El Comprador evaluará y comparará las ofertas que se ajusten a los requisitos de los documentos de licitación.

3.6.6 En el caso de que haya ofertas expresadas en diferentes monedas, a los fines de la evaluación, comparación de precios y adjudicación el Comprador convertirá todos los precios a pesos argentinos, utilizando el tipo de cambio vendedor del Banco de la Nación Argentina, del día hábil anterior a la fecha de apertura de ofertas.

---

### **3.7 Derecho del Comprador a Aceptar Cualquier Oferta y a Rechazar Cualquiera o Todas las Ofertas**

3.7.1 El Comprador se reserva el derecho a aceptar o rechazar cualquier oferta, de anular el proceso licitatorio y de rechazar todas las ofertas en cualquier momento antes de la adjudicación del Contrato, sin que por ello adquiera responsabilidad alguna ante los Licitantes.

### **3.8 Adjudicación del Contrato**

3.8.1 El Contratante adjudicará el Contrato al Licitante cuya Oferta se ajuste a las condiciones y requisitos de estos Documentos y resulte ser la de precio evaluado más bajo, siempre y cuando reúnan los requisitos de post-calificación especificados en el Llamado a Licitación, y en esta cláusula.

Los requisitos de calificación incluyen:

#### **a) Experiencia y Volumen de fabricación y/o comercialización**

##### **Experiencia demostrable en el rubro:**

El licitante deberá haber ejecutado en su totalidad un mínimo de 3 contratos similares a los que son objeto de la presente licitación durante los últimos 2 años. Se entiende por contrato similar a aquel que tenga por objeto desarrollos a medida (bienes como los ofrecidos o similares) en el ámbito de aplicaciones de sistemas autónomos de energías renovables preferentemente. Se acreditará mediante la inclusión en la oferta del listado de ventas indicando como mínimo la siguiente información: cliente, bienes suministrados y cantidades suministradas de dichos bienes o copia de los contratos.

#### **b) Capacidad financiera**

El Licitante deberá demostrar una facturación anual promedio equivalente a:

##### **Lote Nro. 1: ARS 19.824.000.**

(\*). Serán utilizados los siguientes coeficientes de actualización y conversión a moneda local **por parte del contratante en el momento de la evaluación de ofertas.**

Los valores en pesos referidos a los requisitos exigidos 3.8.1 se actualizarán al 1º de enero del año de la apertura de la licitación, utilizando los factores incluidos en la siguiente tabla.

Factor de actualización:

Año 2012: 2,24  
 Año 2013: 1,90  
 Año 2014: 1.67  
 Año 2015: 1.51  
 Año 2016: 1.18

Para los contratos firmados en el exterior y cuyos precios no hayan sido estipulados en pesos, los montos se expresarán en dólares estadounidenses (U\$S) debiendo señalarse el tipo de cambio y fuente. Dicha información será convertida a pesos, de acuerdo a la tabla siguiente y luego actualizada con el factor de actualización señalado up supra:

Valor de conversión a pesos:

Año 2012: 4,53 (valor promedio)  
 Año 2013: 5,55 (valor promedio)  
 Año 2014: 7,99 (valor promedio)  
 Año 2015: 9,47 (valor promedio)  
 Año 2016: 15,19 (valor promedio)

---

\*Fuente: tipo de cambio vendedor del Banco Nación de la República Argentina.

Se acreditará mediante la inclusión de una copia de los balances de los dos (2) últimos estados financieros –personas jurídicas- o declaraciones de ingresos, utilidades y pérdidas –personas físicas- de los dos (2) ejercicios cerrados y auditados con anterioridad a la fecha límite de presentación de oferta.

Se entiende por bienes similares aquellos bienes pertenecientes al mismo rubro o sector que los bienes ofrecidos en la presente licitación.

3.8.2 En caso de presentarse un Consorcio o Asociación de Empresas, la oferta se evaluará en forma conjunta sumando las calificaciones de cada firma.

La información para cada una de las firmas asociadas deberán sumarse para determinar el cumplimiento del Licitante con los criterios mínimos requeridos; sin embargo, para que una firma asociada califique, el socio responsable debe satisfacer por lo menos 40 por ciento de esos criterios mínimos estipulados como criterios para un Licitante individual y los otros socios, al menos, el 25% de estos criterios. El incumplimiento de este requisito podrá dar como resultado el rechazo de la asociación. La experiencia y recursos de los subcontratistas no se tomarán en cuenta para determinar el cumplimiento del Licitante con los criterios establecidos como requisitos.

3.8.3 El Comprador se reserva el derecho, al momento de adjudicar el contrato, de incrementar o reducir las cantidades de los bienes y servicios conexos especificados en los documentos de licitación, siempre y cuando esta variación no exceda el 15% del total de los bienes y servicios y no podrá modificar los precios unitarios y los términos y condiciones de los documentos de licitación y de la Oferta.

### **3.9 Notificación al Adjudicatario**

3.9.1 El Contratante notificará fehacientemente al Adjudicatario, que su oferta ha sido aceptada, para que éste se presente a firmar el Contrato respectivo en el lugar y fecha que determine el Contratante. Si así no lo hiciere en un plazo máximo de quince (15) días o cualquier otro plazo acordado entre las partes, el Contratante procederá a ejecutar el Manifiesto de Garantía de la Oferta.

3.9.2 Mientras se prepara un Contrato formal y es perfeccionado, la notificación de adjudicación constituirá el Contrato.

3.9.3 Dentro de los quince (15) días siguientes al recibo de la notificación de adjudicación de parte del Comprador, el Licitante seleccionado deberá presentar la Garantía de Cumplimiento del Contrato, de conformidad con el formulario de Garantía de Cumplimiento incluido en el Anexo 8, por un monto equivalente al 10% del valor del Contrato.

3.9.4 Cuando el Licitante seleccionado presente la garantía de cumplimiento de conformidad con el Formulario del Anexo 8 y suscriba el contrato, el Comprador informará inmediatamente a cada uno de los licitantes no seleccionados los resultados de la Evaluación de las Ofertas.

3.9.5 La Garantía de Cumplimiento será liberada por el Comprador y devuelta al Proveedor a más tardar treinta (30) días contados a partir de la fecha de recepción definitiva de los bienes.

### **3.10 Firma del Contrato**

3.10.1 El Licitante seleccionado tendrá un plazo de quince (15) días, a partir de la fecha de notificación de adjudicación, para firmar el Contrato.

### **3.11 Garantía de los bienes**

---

- 3.11.1 El Proveedor garantiza que todos los bienes suministrados en virtud del contrato son nuevos, sin uso, y del último modelo a la fecha límite fijada para la presentar ofertas.
- 3.11.2 El Proveedor garantiza además que todos los bienes suministrados en virtud del contrato estarán libres de defectos atribuibles al diseño, los materiales o la confección o a cualquier acto u omisión del Proveedor que pudiera manifestarse en ocasión del uso normal de los bienes en las condiciones imperantes en el país.  
Los bienes deberán poseer una garantía según el plazo indicado en las Especificaciones Técnicas, desde la fecha de recepción de los mismos en el lugar de entrega estipulado.
- 3.11.3 El Comprador notificará de inmediato y por escrito al Proveedor cualquier reclamación a que hubiera lugar con arreglo a la garantía y el Proveedor reparará o reemplazará los bienes defectuosos en todo o en parte, sin costo para el comprador, dentro del plazo máximo de treinta días (30) de notificada la reclamación.

### **3.12 Asociación en Participación o Consorcio**

- 3.12.1 Si el Proveedor es una Asociación en Participación o Consorcio, todas las partes que lo conforman deberán ser mancomunada y solidariamente responsables frente al Comprador por el cumplimiento de las disposiciones del Contrato y deberán designar a una de ellas para que actúe como representante con autoridad para comprometer a la Asociación en Participación o Consorcio. La composición o constitución de la Asociación en Participación o Consorcio no podrá ser alterada sin el previo consentimiento del Comprador.

### **3.13 Ordenes de Cambio y Enmiendas al Contrato**

- 3.13.1 El Comprador podrá, en cualquier momento, efectuar cambios dentro del marco general del Contrato, mediante orden escrita al Proveedor, en uno o más de los siguientes aspectos:
- (a) planos, diseños o especificaciones, cuando los Bienes que deban suministrarse en virtud al Contrato deban ser fabricados específicamente para el Comprador;
  - (b) la forma de embarque o de embalaje;
  - (c) el lugar de entrega, y/o
  - (d) los Servicios Conexos que deba suministrar el Proveedor.
- 3.13.2 Si cualquiera de estos cambios causara un aumento o disminución en el costo o en el tiempo necesario para que el Proveedor cumpla cualquiera de las obligaciones en virtud del Contrato, se efectuará un ajuste equitativo al Precio del Contrato o al Plan de Entregas/de Cumplimiento, o a ambas cosas, y el Contrato se enmendará según corresponda. El Proveedor deberá presentar la solicitud de ajuste de conformidad con esta Cláusula, dentro de los veintiocho (28) días contados a partir de la fecha en que éste reciba la solicitud de la orden de cambio del Comprador.
- 3.13.3 Los precios que cobrará el Proveedor por Servicios Conexos que pudieran ser necesarios pero que no fueron incluidos en el Contrato, deberán convenirse previamente entre las partes, y no excederán los precios que el Proveedor cobra actualmente a terceros por servicios similares.
- 3.13.4 Sujeto a lo anterior, no se introducirá ningún cambio o modificación al Contrato excepto mediante una enmienda por escrito ejecutada por ambas partes.
-

## C. PAÍSES ELEGIBLES

### **Elegibilidad para el suministro de bienes, la contratación de obras y prestación de servicios en adquisiciones financiadas por el Banco**

1. De acuerdo con el párrafo 1.8 de las Normas: Adquisiciones con Préstamos del BIRF y Créditos de la AIF, publicadas por el Banco en mayo de 2004 y revisadas en octubre de 2005 y mayo de 2010, el Banco le permite a firmas e individuos de todos los países suministrar bienes, obras y servicios para proyectos financiados por el Banco. Excepcionalmente, las firmas de un país o los bienes fabricados en un país podrían ser excluidos si:

Párrafo 1.8 (a) (i): por condición de leyes o regulaciones oficiales, el país del Prestatario prohíbe relaciones comerciales con ese País, siempre que el Banco esté de acuerdo con que dicha exclusión no impide la competencia efectiva para la provisión de los Bienes y Obras requeridas; o

Párrafo 1.8(a)(ii): en cumplimiento de una decisión del Consejo de Seguridad de las Naciones Unidas adoptada en virtud del Capítulo VII de la Carta de las Naciones Unidas, el país Prestatario prohíbe la importación de bienes de ese país o pagos de cualquier naturaleza a personas o entidades de ese país.

2. Para información del prestatario y los licitantes, las firmas, bienes y servicios que están excluidos actualmente de participar en esta licitación pueden consultarse en [www.worldbank.org/debarr](http://www.worldbank.org/debarr).

---

## D. CONDICIONES DEL CONTRATO

### 4.1 Lugares y plazos de entrega

4.1.1 Lugar de entrega: **Av. Eduardo Madero 942. Piso 15. Oficinas de PERMER. C1105ACW.**

4.1.2 La entrega considerando la necesidad de adecuar los equipos, los lugares de destino, transporte, e instalación propiamente dicha, que está a cargo del licitante, será de acuerdo al siguiente cronograma:

*Ver detalle descripto en el Anexo 5.*

Para el caso de incumplimiento del plazo establecido, se aplicará al Proveedor una penalidad del 2% sobre el valor de los bienes demorados por cada semana de demora, hasta un máximo del 10% del monto del contrato y podrá ser retenida de los pagos al Proveedor.

### 4.2 Contabilidad, inspección y auditoría por el Banco de los archivos del proveedor.

4.2.1 El Proveedor permitirá al Banco y/u otras personas designadas por el Banco inspeccionar los bienes y servicios, y/o las cuentas y registros del Proveedor y de sus sub-proveedores relativos a la Oferta del Proveedor y la ejecución del contrato, y tener tales cuentas y registros auditados por auditores designados por el Banco, si el Banco así lo exigiera. El Proveedor deberá tener presente lo previsto en la Subcláusula 5.1.1 (b) de las Condiciones del Contrato la cual prevé que todo acto dirigido a impedir de forma material el derecho del Banco a inspeccionar y auditar establecido en la presente Subcláusula constituye una práctica prohibida sujeta a sanción por el Banco.

### 4.3 Inspección y Prueba de los bienes.

4.3.1 Las siguientes inspecciones y pruebas se realizarán:

Inspección definitiva (aceptación definitiva): A la entrega de los bienes en los destinos finales indicados en la Lista de Bienes y Plan de Entregas, el personal designado por el Comprador, verificará los siguientes aspectos:

- (a) Cantidades de artículos, conforme a Lista de Bienes y Plan de Entregas.
- (b) Modelo de los artículos conforme la oferta.
- (c) Origen de los bienes de acuerdo a lo declarado en la oferta.
- (d) Provisión de manuales técnicos y de usuario en español.
- (e) Provisión de certificados de garantía de funcionamiento.
- (f) Defectos externos apreciables (raspaduras, roturas y otros daños físicos evidentes).
- (g) Embalaje conforme a las exigencias de este Documento de Licitación.
- (h) Ensayos conforme lo mencionado en las especificaciones técnicas.
- (i) Se verificará que cada datalogger tenga sus sensores y cables.

Una vez practicadas estas inspecciones, el personal designado por el Comprador emitirá el acta de inspección definitiva. Si alguno de los aspectos precedentes no se hallaran conformes, el personal designado por el Comprador asentará en el acta de inspección definitiva, e implicará para el proveedor el reemplazo de los bienes no conformes dentro del siguiente plazo: 30 (treinta) días.

### 4.4 Pago

4.4.1 El pago de los bienes y servicios se realizará de la siguiente manera:

- (i) **Contra aceptación:** El ciento por ciento (100%) del Precio del Contrato se pagará al Proveedor dentro de los treinta (30) días siguientes a la fecha del certificado de aceptación de la entrega respectiva, emitido por el Comprador.

El pago se efectuará en pesos argentinos (AR\$). El medio de pago a utilizar es la transferencia bancaria directa a la cuenta que indique el Proveedor.

---

El pago se efectuará dentro de los treinta (30) días siguientes a la presentación de una solicitud de pago acompañada de un certificado del Comprador que indique que los bienes han sido recibidos y que todos los demás servicios contratados han sido cumplidos.

#### 4.4.2 Documentación de pago:

- i. Original y copia de la Factura del Proveedor, en la que se describa al Comprador como **Proyecto de Energías Renovables en Mercados Rurales, Préstamo BIRF 8484 -AR del Ministerio de Energía y Minería de La Nación**, la descripción, cantidad, precio unitario y monto total de los bienes.
- ii. Original y copia de la orden del remito en que se describa al Comprador como, **Proyecto de Energías Renovables en Mercados Rurales, Préstamo 8484 -AR del Ministerio de Energía y Minería de la Nación** y con indicación del destino final Av. Eduardo Madero 942. Piso 15. Oficinas PERMER C1105ACW. Ciudad de Buenos Aires. de conformidad con la Lista de Bienes y Servicios y Plan de Entregas.
- iii. Certificado de origen de todos los artículos suministrados, emitido por el Proveedor.
- iv. Certificado de aceptación emitido por el Comprador, para la percepción del pago.

#### 4.5 Intereses por mora en el pago

- 4.5.1 En caso que el Comprador, por causas no imputables al Proveedor, efectuará el pago del bien excediendo el plazo previsto, deberá abonar al Proveedor los intereses correspondientes a los días de atraso, aplicando un 0,5% semanal por cada semana de retraso en el pago.

Los intereses se abonarán sobre la suma líquida o monto neto a pagar al Proveedor.

### 5. Rescisión del contrato

#### 5.1 Rescisión por causa del Proveedor

- 5.1.1 El Comprador tendrá derecho a rescindir el Contrato cuando el Proveedor:

- a. Obre con dolo, culpa grave o reiterada negligencia en el cumplimiento de sus obligaciones.
- b. A juicio del Comprador haya empleado prácticas corruptas, fraudulentas, colusivas, coercitivas u obstructivas al competir por ó en la ejecución del Contrato.

Para propósitos de esta cláusula:

- (i) “práctica corrupta” significa el ofrecimiento, suministro, aceptación o solicitud, directa o indirectamente, de cualquier cosa de valor con el fin de influir impropriamente en la actuación de otra persona<sup>6</sup>;
- (ii) “práctica fraudulenta” significa cualquier actuación u omisión, incluyendo una tergiversación de los hechos que, astuta o descuidadamente, desorienta o intenta desorientar a otra persona con el fin de obtener un beneficio financiero o de otra índole, o para evitar una obligación<sup>7</sup>;

<sup>6</sup> “Persona” se refiere a un funcionario público que actúa con relación al proceso de contratación o la ejecución del contrato. En este contexto, “funcionario público” incluye a personal del Banco Mundial y a empleados de otras organizaciones que toman o revisan decisiones relativas a los contratos.

<sup>7</sup> “Persona” significa un funcionario público; los términos “beneficio” y “obligación” se refieren al proceso de contratación o a la ejecución del contrato; y el término “actuación u omisión” debe estar dirigida a influenciar el proceso de contratación o la ejecución de un contrato.

- (iii) “práctica de colusión” significa un arreglo de dos o más personas<sup>8</sup> diseñado para lograr un propósito impropio, incluyendo influenciar impropriamente las acciones de otra persona;
- (iv) “práctica coercitiva” significa el daño o amenazas para dañar, directa o indirectamente, a cualquiera persona, o las propiedades de una persona, para influenciar impropriamente sus actuaciones<sup>9</sup>.
- (v) “práctica de obstrucción” significa
  - (aa) la destrucción, falsificación, alteración o escondimiento deliberados de evidencia material relativa a una investigación o brindar testimonios falsos a los investigadores para impedir materialmente una investigación por parte del Banco, de alegaciones de prácticas corruptas, fraudulentas, coercitivas o de colusión; y/o la amenaza, persecución o intimidación de cualquier persona para evitar que pueda revelar lo que conoce sobre asuntos relevantes a la investigación o lleve a cabo la investigación, o
  - (bb) las actuaciones dirigidas a impedir materialmente el ejercicio de los derechos del Banco a inspeccionar y auditar de conformidad con la Subcláusula 1.4.1 (e) de la Sección A.

c. No entregar el bien dentro del plazo establecido, superándose el tope de monto de multa establecido.

d. El Comprador podrá rescindir el Contrato mediante comunicación por escrito al Proveedor si éste se declarase en quiebra o en estado de insolvencia. En tal caso, la terminación será sin indemnización alguna para el Proveedor, siempre que dicha terminación no perjudique o afecte algún derecho de acción o recurso que tenga o pudiera llegar a tener posteriormente hacia el Comprador.

## 5.2 Terminación por Conveniencia

5.2.1 El Comprador, mediante comunicación enviada al Proveedor, podrá terminar el Contrato total o parcialmente, en cualquier momento por razones de conveniencia. La comunicación de terminación deberá indicar que la terminación es por conveniencia del Comprador, el alcance de la terminación de las responsabilidades del Proveedor en virtud del Contrato y la fecha de efectividad de dicha terminación.

## 6. Recepción del bien y plazo de garantía

6.1 Una vez recibido el bien de conformidad por la Unidad Ejecutora del Proyecto, se confeccionará un Acta de Recepción del Bien. Asimismo, el personal técnico del Comprador emitirá un certificado de aceptación que permitirá que el Proveedor presente la factura correspondiente. A partir de esta instancia comenzará a regir la garantía del bien.

---

<sup>8</sup> “Personas” se refiere a los participantes en el proceso de contratación (incluyendo a funcionarios públicos) que intentan, por sí mismos o por medio de otra persona o entidad no participante del proceso, establecer precios de oferta a niveles artificiales y no competitivos.

<sup>9</sup> “Persona” se refiere a un participante en el proceso de contratación o en la ejecución de un contrato. —



## **7. Solución de Controversias**

- 7.1 El Comprador y el Proveedor harán todo lo posible para resolver amigablemente mediante negociaciones directas informales, cualquier desacuerdo o controversia que se haya suscitado entre ellos en virtud o en referencia al Contrato.
- 7.2 Si después de transcurridos veintiocho (28) días las partes no han podido resolver la controversia o diferencia mediante dichas consultas mutuas, entonces el Comprador o el Proveedor podrá informar a la otra parte sobre sus intenciones de iniciar un proceso judicial.
- 7.3 Se deja establecido que cualquier contienda que surja de la contratación propiciada, así como también sobre la interpretación de cláusulas contractuales y/o del presente documento, serán dirimidas en los Tribunales Federales con asiento en la Ciudad de Buenos Aires. En consecuencia quién resulte adjudicatario deberá constituir domicilio legal en la Ciudad de Buenos Aires, donde serán válidas todas las notificaciones judiciales o extrajudiciales que deban practicarse.

## E. ESPECIFICACIONES TÉCNICAS

LOTE	DETALLE	<i>Nombre de los Bienes o Servicios Conexos</i>	<i>Cantidad</i>
UNICO	ÍTEM 1	Equipos datalogger para escuelas rurales	500
	ÍTEM 2	Desarrollo de software en soporte físico	1

### 1. Equipo de Datalogger:

#### 1 Introducción

En la presente sección se detallan los requerimientos de hardware (especificaciones eléctricas, interfaces, etc.) y de software (funcionalidades, protocolos de comunicación, etc.) de los datalogger solares a utilizar en las instalaciones fotovoltaicas del PERMER.

La función del datalogger aquí descrito es la de medir el valor de múltiples variables de interés (tensiones, corrientes y temperaturas) en función del tiempo (hora y fecha), filtrarlas, analizarlas y almacenarlas. El mismo contará con una interfaz Ethernet y una interfaz IEEE 802.11 (Wi-Fi), las cuales serán utilizadas para enviar los datos recogidos vía internet o una conexión local (TCP/IP) a un servidor central, utilizando el protocolo que se especifica en este documento.

Cada datalogger contará con una identificación única (ID) la cual será configurable y se utilizará para su individualización y monitoreo.

Asimismo, el datalogger deberá permitir la configuración de distintos tipos de alarma y eventos (valores fuera de un rango especificado, eventos internos y externos, etc.), las cuales serán también almacenadas y reportadas al servidor.

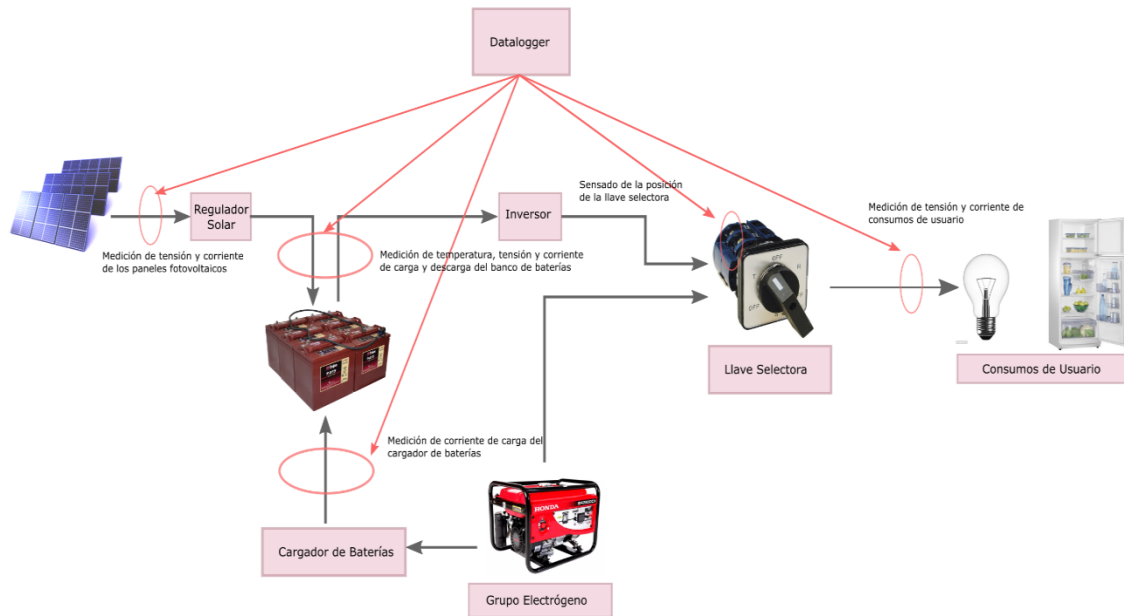
A continuación, se listan las variables a medir por el datalogger (en el desarrollo del documento se ampliarán los detalles y requerimientos de cada medición):

- 1) Tensión de los paneles fotovoltaicos.
- 2) Corriente entregada por los paneles fotovoltaicos.
- 3) Tensión del banco de baterías.
- 4) Corriente de carga y descarga del banco de baterías.
- 5) Corriente entregada por el cargador de baterías al banco de baterías.
- 6) Temperatura del banco de baterías.
- 7) Tensión alterna de consumos de usuario.
- 8) Corriente alterna de consumos de usuario.
- 9) Posición de la llave selectora.

Algunas instalaciones contarán con un grupo electrógeno y una llave selectora para alimentar los consumos del usuario. Normalmente, el grupo alimentará consumos de mayor potencia y cargará baterías a través de un cargador conectado al mismo.

La posición de la llave selectora se determinará utilizando las entradas de contacto seco del datalogger. De esta forma podrá determinarse, ante la falta de tensión en la salida de la llave, si ocurriese algún desperfecto con el inversor o con el grupo electrógeno.

A modo de ejemplo, el siguiente diagrama ilustra los puntos de medición antes listados:



## 2 Descripción Funcional

En esta sección se especificarán distintos aspectos del funcionamiento general de datalogger.

### 2.1.1 Configuración del datalogger vía interfaz Web

El datalogger deberá proveer una interfaz web amigable para la administración de los parámetros de configuración que se especifican en este documento (en forma similar a las interfaces web que proveen los routers o módems comerciales).

Dicha interfaz deberá poder ser accedida tanto a través de la conexión Wi-Fi como de la conexión Ethernet, utilizando un navegador para ingresar a la dirección IP del datalogger en el puerto 80 (HTTP).

Para acceder a todas las páginas deberá utilizarse un usuario y contraseña, los cuales deberán ser modificables a través de la misma interfaz.

Por defecto, los valores serán los siguientes:

- **Nombre de usuario:** admin
- **Contraseña:** admin

**Importante:** Al ingresar por primera vez al datalogger a través de su interfaz web, el mismo deberá forzar el cambio del nombre de usuario y contraseña por defecto de forma tal de evitar posibles problemas de seguridad. Al presionar el pulsador de reset, estos valores deben volver a sus valores por defecto.

#### 2.1.1.1 Página web principal

El datalogger deberá proveer una página web con un resumen de su estado actual (mediciones actuales, eventos, alarmas, estado de conexión, etc.). Dicha página deberá poder ser accedida al ingresar con un navegador web a la siguiente dirección:

[http://ip\\_datalogger/admin.html](http://ip_datalogger/admin.html)

Dicha página será la página principal, y el punto de partida para poder navegar a través de enlaces al resto de las páginas servidas por el datalogger.

#### 2.1.1.2 Página web de reporte de datos

El datalogger deberá proveer la posibilidad de descargar un reporte de datos y mediciones en formato CSV (valores separados por comas, archivo de texto). Para ello, se utilizará la siguiente dirección:

[http://ip\\_datalogger/mediciones.html](http://ip_datalogger/mediciones.html)

En dicha página deberá poder elegirse, mediante una interfaz amigable, la fecha y hora de comienzo y fin del archivo de reporte a descargar. El archivo será un archivo de texto (codificación ANSI) y seguirá el formato de las mediciones especificado en la sección 5.5.3.1, sin los encabezados o "tags" XML.

#### 2.1.1.3 Página web de configuración de red

El datalogger deberá permitir la configuración de los parámetros de red utilizando un navegador web para acceder a la siguiente URL:

[http://ip\\_datalogger/configuracionRed.html](http://ip_datalogger/configuracionRed.html)

En esta página deberá poderse configurar los parámetros de conexión especificados en la sección 3.1.

#### 2.1.1.4 Página web de configuración de mediciones

El datalogger deberá permitir la configuración de los parámetros de las mediciones utilizando un navegador web para acceder a la siguiente URL:

[http://ip\\_datalogger/configuracionMediciones.html](http://ip_datalogger/configuracionMediciones.html)

En esta página deberá poderse configurar los parámetros especificados en la sección 3.3.

#### 2.1.1.5 Página web de configuración de alarmas

El datalogger deberá permitir la configuración de los parámetros de las alarmas utilizando un navegador web para acceder a la siguiente URL:

[http://ip\\_datalogger/configuracionAlarmas.html](http://ip_datalogger/configuracionAlarmas.html)

En esta página deberá poderse configurar los parámetros especificados en la sección 3.4.

---

### 2.1.1.6 Página web de configuración de eventos

El datalogger deberá permitir la configuración de los parámetros de los eventos utilizando un navegador web para acceder a la siguiente URL:

[http://ip\\_datalogger/configuracionEventos.html](http://ip_datalogger/configuracionEventos.html)

En esta página deberá poderse configurar los parámetros especificados en la sección 3.5.

### 2.1.2 Real Time Clock RTC

El datalogger deberá contar con un reloj interno (RTC, Real Time Clock), el cual no deberá perder la hora y fecha al ser desconectada la alimentación. La estabilidad de frecuencia del mismo deberá presentar una variación de 20ppm o menor.

De forma tal de mantener en correcta sincronización la hora y fecha del RTC, el datalogger deberá periódicamente re-sincronizar la hora con el servidor central, enviando el pedido de hora explicado en la sección 5.5.2.

Esta re-sincronización deberá ocurrir por lo menos 1 vez por semana y siempre que el RTC haya perdido su hora por alguna otra razón.

### 2.1.3 Reporte periódico de datos al servidor

El datalogger deberá conectarse periódicamente al servidor central de forma tal de reportar los datos obtenidos a partir de las mediciones (el protocolo de conexión es explicado en la sección 5).

Las variables a reportar periódicamente son:

- 1) Tensión de los paneles fotovoltaicos.
- 2) Corriente entregada por los paneles fotovoltaicos.
- 3) Potencia instantánea entregada por el regulador solar.
- 4) Energía diaria generada por los paneles fotovoltaicos.
- 5) Tensión del banco de baterías.
- 6) Corriente de carga y descarga del banco de baterías.
- 7) Estado de carga del banco de baterías.
- 8) Corriente entregada por el cargador de baterías al banco de baterías.
- 9) Temperatura del banco de baterías.
- 10) Tensión alterna de consumos de usuario.
- 11) Corriente alterna de consumos de usuario.
- 12) Potencia instantánea de CA.
- 13) Energía diaria consumida.
- 14) Posición de la llave selectora.

Los parámetros de conexión al servidor deberán ser configurable mediante la interfaz web de usuario.

**Importante:** Sólo una vez que se confirma el envío exitoso de los datos al servidor podrá el datalogger liberar su memoria interna para guardar nuevos datos. Dicha confirmación será comunicada por el servidor central al enviar el comando de configuración de hora y fecha de próxima conexión (sección 5.6.3).

En caso de perder conexión con el servidor central durante períodos prolongados, el datalogger deberá poseer memoria interna suficiente para guardar los datos obtenidos durante 120 días de medición (para el período de muestras de 1 minuto) antes de sobrescribirlos con datos nuevos.

#### 2.1.3.1 Cálculo de Potencias

En el caso de tensiones alternas, el valor de potencia a reportar será el obtenido de multiplicar el valor de la tensión RMS medida por el valor de la corriente RMS medida.

En el caso de tensiones continuas, el valor de potencia a reportar será el obtenido de multiplicar el valor de la tensión continua medida por el valor de la corriente continua medida.

#### 2.1.3.2 Cálculo de Energías diarias

El datalogger deberá acumular los valores diarios de energía generada y consumida. Para ello deberá “integrar” en forma periódica el valor de potencia correspondiente previamente calculado. El período de integración deberá ser como máximo de 1 minuto.

### 2.1.3.3 Cálculo de Estado de Carga del Banco de Baterías

Para **estimar** el estado de carga del banco de baterías, el datalogger utilizará la tensión medida entregada por el mismo, y corregirá el valor de la misma teniendo en cuenta la temperatura del banco (independientemente de la corriente de carga o descarga instantánea). Con este valor de tensión corregido por temperatura, el datalogger deberá reportar el estado de carga del banco en rangos del 20%, es decir:

- **Nivel 1 (muy bajo):** 0% - 20%
- **Nivel 2 (bajo):** 21% - 40%
- **Nivel 3 (medio):** 41% - 60%
- **Nivel 4 (alto):** 61% - 80%
- **Nivel 5 (muy alto):** 81% - 100%

Deberá ser posible configurar los rangos de tensiones (sección 3.3.3) correspondientes a cada nivel en forma manual a través de la interfaz web y en forma automática a través del comando de configuración de mediciones del servidor central descrito en la sección 3.3.

### 2.1.4 Reporte de alarmas y eventos al servidor central

El datalogger deberá detectar eventos o anomalías en los valores de las variables a reportar antes mencionadas: por ejemplo, cuando alguna de las variables no se encuentre dentro de un rango determinado (por un período de tiempo definido), el datalogger deberá generar una alarma y reportarla inmediatamente al servidor central. Igualmente, al normalizarse la condición de alarma, el datalogger deberá detectar y reportar dicho cambio.

En forma similar a las mediciones, las alarmas y eventos deberán ser guardadas en la memoria interna y ser reportadas durante el reporte periódico de mediciones. De esta forma, si durante una alarma el datalogger no posee una conexión a internet, la información del evento no es descartada, sino que se reportará en la próxima conexión al servidor.

Las alarmas a reportar son las siguientes:

- 1) Alarma de baja tensión en el banco de baterías.
- 2) Alarma de sobretensión en el banco de baterías.
- 3) Alarma de sobrecorriente de carga del regulador solar en el banco de baterías.
- 4) Alarma de sobrecorriente de carga del cargador de baterías.
- 5) Alarma de sobrecorriente de descarga en el banco de baterías.
- 6) Alarma de potencia diurna nula en el regulador solar.
- 7) Alarma de potencia nula a la salida del inversor.
- 8) Alarma de sobrecorriente en la salida del inversor.
- 9) Alarma de alta temperatura en el banco de baterías.
- 10) Alarma de baja temperatura en el banco de baterías.

Los rangos válidos (y de alarma) de estas variables, así como también la duración mínima durante la cual debe sostenerse la situación anómala para generar una alarma, deberán ser configurables (sección 3.4) a través de la interfaz web del datalogger y en forma automática por el servidor central, siguiendo el protocolo especificado en la sección 5. Asimismo, las alarmas podrán ser habilitadas o inhabilitadas por los mismos mecanismos.

Los eventos que el datalogger debe detectar y reportar automáticamente son:

- 1) Encendido del sistema.
  - 2) Apagado del sistema.
  - 3) Reseteo del sistema por watchdog interno.
  - 4) Reseteo del sistema por watchdog externo.
  - 5) Reseteo a valores por defecto.
  - 6) Conexión a la red (Wi-Fi o Ethernet).
  - 7) Desconexión de la red (Wi-Fi o Ethernet).
  - 8) Alarma de baja memoria interna disponible debido a pérdida de conexión prolongada.
  - 9) Alarma de pérdida de datos y mediciones debido a desconexión prolongada.
-

**Importante:** Sólo una vez que se confirma el envío exitoso de las alarmas y eventos al servidor central podrá el datalogger borrarlos de su memoria interna. Dicha confirmación será comunicada por el servidor central al enviar el comando de configuración de hora y fecha de próxima conexión (sección 5.6.3).

En caso de perder conexión con el servidor central durante períodos prolongados, el datalogger deberá poseer memoria interna suficiente para guardar 500 alarmas y eventos antes de sobrescribirlos con nuevos datos.

### 2.1.5 Indicadores Luminosos (LEDs) y pulsadores

El datalogger deberá contar con indicadores luminosos (LEDs) que indiquen:

- Estado del datalogger: Encendido/Apagado.
- Estado de conexión Wi-Fi: conectado/desconectado.
- Estado de conexión Ethernet: conectado/desconectado.

Asimismo, el datalogger deberá contar con un pulsador de encendido/apagado y un pulsador de difícil acceso para resetear la configuración a los valores por defecto. Ambos pulsadores deberán ser del tipo “momentáneos”, es decir que sólo se mantendrán activados durante la presión ejercida por el usuario.

### 2.1.6 Encendido/Apagado, arranque y estabilidad del sistema

El datalogger deberá poder ser apagado en cualquier momento sin que el mismo pierda su configuración o los datos de mediciones guardados en su memoria interna. Será de especial importancia la robustez del datalogger respecto a desconexiones de su fuente de alimentación o reseteos por parte del usuario, ya que deberá garantizarse que los datos medidos no sean corrompidos. Ante tales casos el datalogger deberá haber guardado en su memoria interna en forma segura los datos medidos hasta 5 minutos antes de la desconexión.

En caso de detectarse una desconexión inesperada, o un reseteo, el datalogger deberá guardar en su memoria dicho evento cuando vuelva a ser encendido.

Al ser encendido, y sin importar la causa previa de apagado, el datalogger deberá comenzar a funcionar en forma automática, sin presentar problemas y reconectarse automáticamente a la red seleccionada en su configuración.

En todos los casos el tiempo de arranque del datalogger deberá ser menor a 3 minutos.

El sistema debe ser estable. Su operación debe ser 100% autónoma y deberá recuperarse de errores de software, conexión y otros. Se recomienda encarecidamente el uso de “Watchdogs”, interno y externo (por hardware), que monitoreen la correcta ejecución del software del sistema.

**Importante:** El datalogger deberá monitorear la tensión de alimentación obtenida desde las baterías. Al detectar que dicha tensión se encuentre por debajo del mínimo necesario para su correcto funcionamiento, el mismo deberá apagarse automáticamente en forma segura y sin perder datos. El datalogger volverá a encenderse al ser presionado el pulsador de encendido/apagado.

### 2.1.7 Actualizaciones de Firmware

De forma tal de facilitar el proceso de desarrollo y de mejora de las terminales, el datalogger deberá proveer la funcionalidad de actualizar su firmware mediante la conexión al servidor central (ya sea a través de la conexión Wi-Fi o la conexión Ethernet). Es de vital importancia que en caso de fallar la transmisión de la actualización el datalogger conserve el firmware previo a iniciar dicho proceso. En ninguna circunstancia el datalogger deberá dejar de cumplir con su correcto funcionamiento.

---

### 3 Parámetros de Configuración

En esta sección se definirán los parámetros que deberán ser configurables del datalogger.

#### 3.1 Configuración de Conexión

Como se especificó anteriormente, el datalogger deberá poseer dos interfaces de red: una Ethernet y la otra Wi-Fi.

La configuración de conexión de red deberá ser modificable a través de la página web de configuración (en forma similar a los routers comerciales) y a través del comando de configuración de red (5.6.4) del servidor central.

El datalogger deberá implementar un cliente DHCP para obtener automáticamente su configuración de red (IP, Puerta de Enlace, máscara de subred y servidores DNS) y responder a mensajes ICMP (ping). Todas las comunicaciones entre las terminales y el servidor central se transmitirán utilizando TCP/IP, según el protocolo que se describe en la sección 5.

**Importante:** Por defecto, la interfaz Ethernet tendrá prioridad sobre la interfaz Wi-Fi: es decir, si el datalogger detecta que está conectado mediante Ethernet, no deberá intentar conectarse a la red Wi-Fi. Caso contrario, intentará conectarse a la red Wi-Fi. No obstante, deberá poder seleccionarse cuál de las dos interfaces se deberá utilizar para conectarse con el servidor central.

##### 3.1.1 ID y contraseña para conexión al servidor central

El datalogger deberá poseer una identificación (ID) y una contraseña, los cuales serán utilizados para conectarse con el servidor central. Los mismos deben poder ser configurados a través de la página web de configuración.

Es importante remarcar que tanto el ID como la contraseña serán del tipo **alfanuméricos y no podrán contener caracteres especiales**, ya que sus valores se utilizarán como parámetros en la URLs de los reportes entre el datalogger y el servidor central.

**Nota:** no deberán confundirse las credenciales para conectarse con el servidor central con el nombre y usuario y contraseña utilizados para acceder a la interfaz web del datalogger.

**Importante:** Al presionar el pulsador de reset, el ID y la contraseña **NO** deberán ser vueltos a los valores por defecto.

##### 3.1.2 Configuración de Red Ethernet

El datalogger deberá proveer la funcionalidad de configurar los siguientes parámetros de conexión a la red Ethernet:

- Selección entre IP estática y cliente DHCP.
- IP de la Puerta de enlace (Gateway).
- Máscara de subred (Netmask).
- DNS Primario.
- DNS Secundario.

**Importante:** Al presionar el pulsador de reset, estos valores deben volver a sus valores por defecto:

- **IP estática:** 192.168.0.100
- **IP de la puerta de enlace:** 192.168.0.1
- **Máscara de subred:** 255.255.255.0
- **DNS Primario:** 8.8.8.8
- **DNS Secundario:** 4.4.4.4

##### 3.1.3 Configuración de Red Wi-Fi

El datalogger deberá proveer la funcionalidad de configurar los siguientes parámetros de conexión a la red Wi-Fi:

- Nombre de la red Wi-Fi (SSID).
  - Tipo de seguridad (Ninguna, WEP, WPA y WPA2).
  - Contraseña.
  - Selección entre IP estática y cliente DHCP.
  - IP de la Puerta de enlace (Gateway).
  - Máscara de subred (Netmask).
-



- DNS Primario.
- DNS Secundario.

**Importante:** Al presionar el pulsador de reset, estos valores deben volver a sus valores por defecto:

- **Nombre de la red:** Ninguno
- **Tipo de seguridad:** Ninguna
- **Contraseña:** Ninguna
- **IP estática:** 192.168.0.101
- **IP de la puerta de enlace:** 192.168.0.1
- **Máscara de subred:** 255.255.255.0
- **DNS Primario:** 8.8.8.8
- **DNS Secundario:** 4.4.4.4

### 3.1.4 Configuración de conexión con el servidor central

En la pantalla de configuración deberán poder configurarse los parámetros de conexión al servidor central:

- IP (o URL) del servidor central.
- Puerto TCP del servidor central.
- Tiempo de espera para establecer la conexión (timeout de conexión).
- Tiempo máximo sin intercambiar datos durante la conexión (timeout de inactividad).
- Cantidad de reintentos de conexión por ciclo.
- Tiempo de espera entre reconexiones.
- Tiempo de espera para recomienzo de ciclo de conexión.

Los valores por defecto de estos parámetros serán:

- **IP (o URL) del servidor central:** a definir.
- **Puerto TCP del servidor central:** 80.
- **Tiempo de espera para establecer la conexión (timeout de conexión):** 60 segundos.
- **Tiempo máximo sin intercambiar datos durante la conexión (timeout de inactividad):** 120 segundos.
- **Cantidad de reintentos de conexión por ciclo:** 5.
- **Tiempo de espera entre reconexiones:** 120 segundos.
- **Tiempo de espera para recomienzo de ciclo de conexión:** 7200 segundos (120 minutos).

### 3.2 Configuración del router/modem para la conexión a internet

El datalogger obtendrá su acceso a internet (vía Ethernet o Wi-Fi), a través de un router o modem, el cual deberá permitir realizar conexiones salientes al servidor central.

Bajo el protocolo planteado, las conexiones son siempre iniciadas por el datalogger, por lo que el router únicamente deberá posibilitar (i.e., no bloquear) conexiones salientes provenientes del datalogger con destino a la IP del servidor central en el puerto especificado. De esta manera, no es necesario abrir o “forwardear” puertos del router hacia el datalogger.

**Nota:** Por simplicidad, se recomienda deshabilitar todas las restricciones de conexiones salientes originadas por el datalogger.

### 3.3 Configuración de Mediciones

El datalogger deberá permitir configurar ciertos parámetros de las mediciones y los cálculos que debe realizar. Estos valores deberán poder ser configurados a través de la página web de configuración y a través del comando de configuración de mediciones (sección 3.3) del servidor central.

#### 3.3.1 Período de medición en reportes

El datalogger deberá permitir configurar el período entre registro de mediciones, las cuales luego serán reportadas al servidor central. Este período deberá ser seleccionable entre: 1 minuto, 5 minutos, 15 minutos, 30 minutos y 60 minutos. Por defecto este valor será de 1 minuto. \_\_\_\_\_

Vale aclarar que si bien este será el período con el que se registrarán en la memoria interna las mediciones y las variables calculadas, el datalogger deberá tomar muestras a mayor velocidad y aplicar el algoritmo de promedio explicado en la sección 4.4.

**Importante:** Al presionar el pulsador de reset **NO** se deberá volver al valor por defecto.

### 3.3.2 Selección de la tensión del banco de baterías

El datalogger deberá permitir seleccionar la tensión del banco de baterías entre los siguientes valores: 12V, 24V y 48V. Por defecto el valor será de 48V.

**Importante:** Al presionar el pulsador de reset **NO** se deberá volver al valor por defecto.

### 3.3.3 Rango de tensiones de carga del banco de baterías

De forma tal de reportar el estado de carga del banco se deberá especificar el valor máximo de tensión para cada rango de carga:

- Tensión máxima para estado “Muy Bajo”.
- Tensión máxima para estado “Bajo”.
- Tensión máxima para estado “Medio”.
- Tensión máxima para estado “Alto”.

Por defecto estos valores serán:

- **Tensión máxima para estado “Muy Bajo”:** 46V
- **Tensión máxima para estado “Bajo”:** 47.6V
- **Tensión máxima para estado “Medio”:** 48.6V
- **Tensión máxima para estado “Alto”:** 49.2V

**Importante:** Al presionar el pulsador de reset **NO** se deberá volver a los valores por defecto.

### 3.3.4 Coeficiente de corrección de tensión de banco de baterías por temperatura

Los valores de tensión con los que se determinará el estado de carga del banco deberán estar corregidos por temperatura (tomando como referencia 25 °C), utilizando un factor de corrección configurable.

Por defecto este valor es de: -3mV/D°C por cada celda.

**Importante:** Al presionar el pulsador de reset **NO** se deberá volver al valor por defecto.

## 3.4 Configuración de Alarmas

El datalogger deberá permitir configurar los parámetros de las distintas condiciones de alarma y de los eventos que debe registrar. Se registrará la ocurrencia de las alarmas así como también el restablecimiento de las condiciones normales. El datalogger deberá comunicar al servidor centra las ocurrencias de estas condiciones en forma inmediata.

Asimismo, cada alarma deberá poder ser habilitada o deshabilitada. Estos valores deberán poder ser configurados a través de la página web de configuración y a través del comando de configuración de alarmas (sección 5.6.6) del servidor central.

**Importante:** En todos los casos, al presionar el pulsador de reset **NO** se deberá volver a los valores configurados por defecto.

### 3.4.1 Configuración de alarma de baja tensión en el banco de baterías

El datalogger deberá detectar cuando la tensión del banco de baterías se mantenga por debajo del valor mínimo configurado durante un período de tiempo establecido. Se registrará la normalización de dicha condición cuando el valor de tensión supere un valor configurable, y dicha condición se sostenga por un período de tiempo (también configurable).

Los parámetros de esta alarma son:

- Tensión de alarma de baja batería.
  - Tiempo mínimo de condición para disparar la alarma (en segundos).
  - Tensión de restablecimiento de condiciones normales.
  - Tiempo mínimo de condiciones normales para restablecimiento de la alarma (en segundos).
  - Alarma habilitada/deshabilitada.
-

### **3.4.2 Alarma de sobretensión en el banco de baterías**

El datalogger deberá detectar cuando la tensión del banco de baterías se mantenga por encima del valor máximo configurado durante un período de tiempo establecido. Se registrará la normalización de dicha condición cuando el valor de tensión sea inferior a un valor configurable, y dicha condición se sostenga por un período de tiempo (también configurable).

Los parámetros de esta alarma son:

- Tensión de alarma de sobre tensión de banco de baterías.
- Tiempo mínimo de condición para disparar la alarma (en segundos).
- Tensión de restablecimiento de condiciones normales.
- Tiempo mínimo de condiciones normales para restablecimiento de la alarma (en segundos).
- Alarma habilitada/deshabilitada.

### **3.4.3 Alarma de sobrecorriente de carga del regulador solar en el banco de baterías**

El datalogger deberá detectar cuando la corriente de carga del regulador solar se mantenga por encima del valor máximo configurado durante un período de tiempo establecido. Se registrará la normalización de dicha condición cuando el valor de corriente de carga de regulador solar sea inferior a un valor configurable y dicha condición se sostenga por un período de tiempo (también configurable).

Los parámetros de esta alarma son:

- Corriente máxima de carga del regulador solar.
- Tiempo mínimo de condición para disparar la alarma (en segundos).
- Corriente de carga del regulador solar para volver a condiciones normales.
- Tiempo mínimo de condiciones normales para restablecimiento de la alarma (en segundos).
- Alarma habilitada/deshabilitada.

### **3.4.4 Alarma de sobrecorriente de carga del cargador de baterías.**

El datalogger deberá detectar cuando la corriente de carga del cargador de baterías se mantenga por encima del valor máximo configurado durante un período de tiempo. Se registrará la normalización de dicha condición cuando el valor de corriente de carga sea inferior a un valor configurable, y dicha condición se sostenga por un período de tiempo.

Los parámetros de esta alarma son:

- Corriente máxima de carga del cargador.
- Tiempo mínimo de condición para disparar la alarma (en segundos).
- Corriente de carga del regulador para volver a condiciones normales.
- Tiempo mínimo de condiciones normales para restablecimiento de la alarma (en segundos).
- Alarma habilitada/deshabilitada.

### **3.4.5 Alarma de sobrecorriente de descarga en el banco de batería**

El datalogger deberá detectar cuando la corriente de descarga del banco de baterías (consumida por el inversor) se mantenga por encima del valor máximo configurado durante un período de tiempo. Se registrará la normalización de dicha condición cuando el valor de corriente de descarga sea inferior a un valor configurable, y dicha condición se sostenga por un período de tiempo.

Los parámetros de esta alarma son:

- Corriente de descarga máxima.
- Tiempo mínimo de condición para disparar la alarma (en segundos).
- Corriente de descarga para volver a condiciones normales.
- Tiempo mínimo de condiciones normales para restablecimiento de la alarma (en segundos).
- Alarma habilitada/deshabilitada.

### **3.4.6 Alarma de potencia diurna nula en el regulador solar**

El datalogger deberá detectar cuando la potencia entregada por el regulador solar sea menor a un valor configurable durante un horario "diurno" especificado. De esta forma se detectarán problemas de funcionamiento de los paneles solares y/o del regulador solar. Se registrará la normalización de

---

dicha condición cuando el valor de potencia entregada por el regulador solar sea mayor un valor configurable, y dicha condición se sostenga por un período de tiempo.

Los parámetros de esta alarma son:

- Potencia mínima entregada por el regulador solar.
- Tiempo mínimo de condición para disparar la alarma (en segundos).
- Potencia entregada por el regulador solar para volver a condiciones normales.
- Tiempo mínimo de condiciones normales para restablecimiento de la alarma (en segundos).
- Hora de comienzo del horario diurno.
- Hora de finalización del horario diurno.
- Alarma habilitada/deshabilitada.

#### **3.4.7 Alarma de potencia nula a la salida del inversor**

El datalogger deberá detectar cuando, con el inversor entregando tensión (es decir, esté encendido), la potencia a la salida del inversor sea menor a un valor configurable durante un período determinado. Se registrará la normalización de dicha condición cuando el valor de potencia entregada por el inversor sea mayor un valor configurable, y dicha condición se sostenga por un período de tiempo.

Los parámetros de esta alarma son:

- Potencia mínima entregada por el inversor.
- Tiempo mínimo de condición para disparar la alarma (en segundos).
- Potencia entregada por el inversor para volver a condiciones normales.
- Tiempo mínimo de condiciones normales para restablecimiento de la alarma (en segundos).
- Alarma habilitada/deshabilitada.

#### **3.4.8 Alarma de sobrecorriente en la salida del inversor**

El datalogger deberá detectar cuando la corriente a la salida del inversor sea mayor a un valor configurable durante un período determinado, de forma tal de detectar sobreconsumos. Se registrará la normalización de dicha condición cuando el valor de corriente entregada por el inversor sea menor un valor configurable, y dicha condición se sostenga por un período de tiempo.

Los parámetros de esta alarma son:

- Corriente máxima entregada por el inversor.
- Tiempo mínimo de condición para disparar la alarma (en segundos).
- Corriente entregada por el inversor para volver a condiciones normales.
- Tiempo mínimo de condiciones normales para restablecimiento de la alarma (en segundos).
- Alarma habilitada/deshabilitada.

#### **3.4.9 Alarma de alta temperatura en el banco de batería**

El datalogger deberá detectar cuando la temperatura del banco de baterías sea mayor a un valor configurable durante un período determinado. Se registrará la normalización de dicha condición cuando el valor la temperatura medida sea menor un valor configurable, y dicha condición se sostenga por un período de tiempo.

Los parámetros de esta alarma son:

- Temperatura máxima en el banco de baterías.
- Tiempo mínimo de condición para disparar la alarma (en segundos).
- Temperatura en el banco de baterías para volver a condiciones normales.
- Tiempo mínimo de condiciones normales para restablecimiento de la alarma (en segundos).
- Alarma habilitada/deshabilitada.

#### **3.4.10 Alarma de baja temperatura en el banco de baterías**

El datalogger deberá detectar cuando la temperatura del banco de baterías sea menor a un valor configurable durante un período determinado. Se registrará la normalización de dicha condición cuando el valor la temperatura medida sea mayor un valor configurable, y dicha condición se sostenga por un período de tiempo.

Los parámetros de esta alarma son:

---

- Temperatura mínima en el banco de baterías.
- Tiempo mínimo de condición para disparar la alarma (en segundos).
- Temperatura en el banco de baterías para volver a condiciones normales.
- Tiempo mínimo de condiciones normales para restablecimiento de la alarma (en segundos).
- Alarma habilitada/deshabilitada.

### 3.5 Configuración de eventos

El datalogger deberá permitir la configuración de los eventos a registrar y reportar al servidor central. Asimismo, el reporte de cada evento deberá poder ser habilitado o deshabilitado. Estos valores deberán poder ser configurados a través de la página web de configuración y a través del comando de configuración de eventos (sección 5.6.7) del servidor central.

#### 3.5.1 Encendido del sistema

El datalogger deberá reportar el evento de encendido de sistema. Si en ese momento no hubiera conectividad presente, el datalogger deberá registrar dicho evento para luego reportarlo al servidor central en la próxima conexión.

Los parámetros de este evento son:

- Reporte de evento habilitado/deshabilitado.

#### 3.5.2 Apagado del sistema

Al desconectarse la alimentación del datalogger, y antes de apagarse por completo, el datalogger deberá guardar en su memoria interna la fecha y hora de la pérdida de alimentación. Dicho evento deberá ser reportado al servidor central en la próxima conexión.

Los parámetros de este evento son:

- Reporte de evento habilitado/deshabilitado.

#### 3.5.3 Reseteo del sistema por watchdog interno

En el caso de que el software del datalogger falle en su ejecución continua, y el watchdog interno haga un reseteo del mismo, el datalogger deberá detectar dicho evento y reportarlo al servidor central una vez que se haya restablecido su funcionamiento normal.

Los parámetros de este evento son:

- Reporte de evento habilitado/deshabilitado.

#### 3.5.4 Reseteo del sistema por watchdog externo

En el caso de que el software del datalogger falle en su ejecución continua, y el watchdog externo haga un reseteo del mismo, el datalogger deberá detectar dicho evento y reportarlo al servidor central una vez que se haya restablecido su funcionamiento normal.

Los parámetros de este evento son:

- Reporte de evento habilitado/deshabilitado.

#### 3.5.5 Reseteo a valores por defecto

El datalogger deberá detectar y comunicar el evento en el caso de que el usuario presione el pulsador de reset oculto para volver a la configuración por defecto. Este evento será reportado al servidor central una vez que la comunicación con el mismo sea restablecida.

Los parámetros de este evento son:

- Reporte de evento habilitado/deshabilitado.

#### 3.5.6 Conexión a la red (Wi-Fi o Ethernet)

El datalogger deberá detectar y comunicar el evento de conexión a la red Wi-Fi o Ethernet. Este evento será reportado al servidor central una vez que la comunicación con el mismo sea restablecida.

Los parámetros de este evento son:

- Reporte de evento habilitado/deshabilitado.

#### 3.5.7 Desconexión de la red (Wi-Fi o Ethernet)

El datalogger deberá detectar y registrar el evento de desconexión a la red Wi-Fi o Ethernet. Este evento será reportado al servidor central una vez que la comunicación con el mismo sea restablecida.

Los parámetros de este evento son:

- Reporte de evento habilitado/deshabilitado.

### 3.5.8 Baja memoria interna disponible debido a pérdida de conexión prolongada

El datalogger deberá detectar y comunicar cuando el espacio libre de su memoria interna sea menor que el valor configurado especificado en kBytes.

Los parámetros de este evento son:

- Espacio libre mínimo en kBytes.
- Reporte de evento habilitado/deshabilitado.

### 3.5.9 Pérdida de datos y mediciones debido a desconexión prolongada

En el caso de que el datalogger haya perdido conectividad con el servidor central por períodos prolongados, y que los datos guardados en su memoria interna hayan tenido que ser sobrescritos con nuevos datos, el mismo deberá registrar dicho evento y reportarlo al servidor central en la próxima conexión con el mismo.

Los parámetros de este evento son:

- Reporte de evento habilitado/deshabilitado.

## 4 Especificaciones de Hardware

### 4.1 Requerimientos Eléctricos

En esta sección se especificarán los requerimientos eléctricos a cumplir por el datalogger:

#### 4.1.1 Alimentación y Consumo

El datalogger se alimentará del banco de baterías del sistema. Para ello, el rango de tensión de alimentación será de 10V-75VCC. La potencia consumida por el mismo deberá ser menor a 5W durante las mediciones y podrá llegar a 8W durante el envío de datos vía Wi-Fi. En total el datalogger no deberá consumir más de 120Wh por día. La alimentación deberá poseer un fusible de protección, de forma tal de evitar posibles incendios ante cortocircuitos o fallas.

**Importante:** La alimentación del datalogger sólo podrá compartir su referencia de potencial (polo positivo), con las mediciones de tensión continua de baterías y de paneles solares. La medición de tensión y corriente alterna de consumos de usuario (salida del inversor), deberán estar aisladas galvánicamente de dicha alimentación. Bajo ninguna condición de tensión de alimentación y estado de carga del banco de baterías, la fuente de alimentación del datalogger deberá inducir ruido en las mediciones de forma tal que se supere la tolerancia especificada en cada caso.

**Nota:** El gabinete del datalogger deberá poseer un borne de “masa”, el cual estará conectado eléctricamente a la tierra del sistema. Dicho borne estará conectado internamente a la malla de los cables de medición, de forma tal de actuar como una pantalla electromagnética ante el ruido eléctrico. **Al diseñar los circuitos, se deberá tener en cuenta que en las instalaciones del proyecto el borne positivo de las baterías estará puesto a tierra mediante una jabalina.**

#### 4.1.2 Interfaces de Comunicación

El datalogger deberá poseer una interfaz Ethernet (RJ45) de 100Mbit para comunicarse con la red local o con una computadora en una conexión punto a punto. El módulo Ethernet utilizado deberá presentar aislación galvánica de forma tal de evitar problemas entre los equipos interconectados. Asimismo, el datalogger deberá poder conectarse como cliente a una red Wi-Fi 802.11 b/g/n en 2.4GHz.

Los detalles de la configuración de dichas interfaces son explicados en la sección 3.1 .

##### 4.1.2.1 Especificaciones de la interfaz Wi-Fi

La interfaz Wi-Fi del datalogger deberá cumplir con las siguientes especificaciones:

- **Tipo de Wi-Fi:** 802.11 b/g/n.
  - **Canales soportados:** 1-11 (2.412GHz-2.462GHz).
  - **Ancho de banda de canal:** 20 MHz.
  - **Potencia de transmisión mínima:** 18dBm (1Mbps, 802.11b), 15 dBm (54Mbps, 802.11 g), 15 dBm, HT20, 802.11n).
-

- **Sensibilidad máxima del receptor:** -90dBm (802.11b @8%PER), -73dBm (802.11g @10%PER), -71 dBm (802.11n @10%PER).
- **Seguridad:** WPA/WP2, 64/128/152-bit WEP.
- **Velocidades de transmisión:**
  - **802.11b:** 1,2, 5.5 y 11Mbps.
  - **802.11g:** 6,9,12,18,24,36,48, 54 Mbps.
  - **802.11n (20MHz):** hasta 72 Mbps.

**Importante:** deberá ser posible conectar una antena externa del tipo dipolo (para 2.4GHz, similar a la de los routers comerciales) para extender el rango de alcance del datalogger.

#### 4.1.3 Entradas de contacto seco

El datalogger deberá contar con por lo menos dos entradas digitales de contacto seco, las cuales reconocerán un circuito abierto (como un 0) o un circuito cerrado (como un 1). La tensión presente en dichas entradas con el contacto abierto no superará los 5V y la corriente con el contacto cerrado deberá ser mayor a 0.1mA y menor o igual a 1mA.

**Importante:** Debido a que estas entradas estarán conectadas a la llave selectora, las mismas deberán contar con protecciones contra tensión inversa, de forma tal de resistir la inyección errónea de tensión alterna (por ejemplo, del tipo varistor con un fusible en serie). Asimismo, deberán contar con filtros “anti-rebote” (ya sea implementados por Hardware o Software), para evitar el sensado incorrecto de los rebotes característicos de los interruptores mecánicos.

#### 4.1.4 Entrada para sensor de temperatura

El datalogger contará con una entrada analógica para sensores de temperatura del tipo NTC (de 10Kohms a 25°C). La tensión con la que se alimentará el sensor no deberá ser mayor o igual a 5V y no deberá superar los 24V. La corriente máxima admisible por el sensor a 25°C será de 0.25mA, de forma tal de evitar errores de medición por el auto-calentamiento del sensor.

#### 4.1.5 Protecciones en entradas

Todas las entradas del datalogger deberán contar con protecciones por sobretensión y sobrecorriente. Los valores se especifican para cada medición en la sección 4.4.

### 4.2 Requerimientos Físicos y Ambientales

El datalogger deberá poder operar en un rango de temperaturas desde -15 °C a 60 °C. El grado de protección del mismo deberá ser por lo menos IP22. La humedad relativa soportada deberá ser mayor al 85% sin condensación.

El datalogger deberá tener un peso máximo de 2 kg y sus dimensiones no deben exceder un cubo de 25x25x25 cm (sin considerar la antena de Wi-Fi externa). El gabinete podrá ser plástico, pero deberá contar con un borne de “masa” para conectarlo eléctricamente a la tierra del sistema.

### 4.3 Resumen de requerimientos eléctricos y de hardware

La siguiente tabla se presenta a modo de resumen de las especificaciones antes explicadas:

Requerimiento	Valores
Alimentación	10-75VCC. Aislada galvánicamente de las entradas de medición de tensión y corriente alterna. Fusible de protección.
Potencia consumida	Menor a 5W, con picos de 8W durante transmisión Wi-Fi.
Consumo energético	Menor a 120Wh/día.
Interfaces de Comunicación	Ethernet 100Mbit, con aislación galvánica. Wi-fi 802.11b/g/n 2.4GHz.
Entradas de contacto seco	2 entradas. Corriente: 0.1mA - 1mA. Tensión máxima en las entradas: 5V. Protección contra inyección de tensión inversa. Filtro “anti-rebote” por hardware o software.
Entrada para sensor de Temperatura	Tipo NTC, 10K a 25°C. Tensión máxima 24V. Corriente máxima 0.25mA a 25°C.
Temperatura de trabajo	-15 °C a 60 °C.

Humedad relativa de trabajo	Hasta 85% sin condensación.
Grado de protección	Mínimo IP22.
Peso máximo	2 kg.
Dimensiones máximas	25x25x25 cm.

#### 4.4 Mediciones

En esta sección se detallarán los requerimientos de cada medición que el datalogger deberá realizar. La frecuencia de muestreo de todas las mediciones deberá ser tal que permita obtener por lo menos 1 muestra por segundo. El datalogger luego procesará las muestras para obtener un valor resultante una vez por minuto. Este valor resultante se obtendrá promediando los valores medidos, luego de descartar los valores erróneos de las mediciones utilizando un filtro digital del tipo "Hampel" (donde las muestras que se alejan por más de tres desvíos estándar de la media son reemplazadas por el valor de dicha media).

**Importante:** En todos los casos que sea necesario utilizar sensores, los mismos deberán ser provistos por el fabricante de forma tal de asegurar la compatibilidad y el correcto funcionamiento con el datalogger. Esto significa que en el caso de necesitar los sensores alimentación externa, la misma deberá ser provista por el datalogger.

##### 4.4.1 Unidades y precisión de las mediciones

Las mediciones se medirán y reportarán en las siguientes unidades y con la siguiente precisión:

Medición	Unidad	Precisión
Tension	Volt	dos decimales
Corriente	Amper	dos decimales
Potencia	Watt	dos decimales
Energía	Watt-Hora	dos decimales
Temperatura	Grados celsius	un decimal
Tiempo	segundos	unidad
Booleano	"true" ó "false"	-
Estado del banco de baterías	0=muy bajo, 1=bajo, 2=medio, 3=alto, 4=muy alto	-
Posición de la llave selectora	0=sin conexión,1=Inversor, 2=Generador	-
Espacio en memoria	kB	-

##### 4.4.2 Tensión de los paneles fotovoltaicos

La tensión continua entregada por los paneles fotovoltaicos a la entrada del regulador de carga solar deberá ser medida. El rango de valores que deberá poder medirse es de 0 a 160 VCC. La medición deberá tener un error menor o igual al 1%. La entrada deberá estar protegida por sobretensiones de hasta 200V, y no deberá consumir más de 10mA para el mayor valor de tensión a medir. Deberá también, contar con un fusible de protección para evitar riesgos de incendio. Se recomienda el uso de un amplificador de instrumentación con alta impedancia de entrada para minimizar corrientes de fuga.

##### 4.4.3 Corriente entregada por los paneles fotovoltaicos

La corriente continua de entrada al regulador de carga solar deberá ser medida por el datalogger. El rango de valores que deberá poder medirse es de 0 a 300 A. La medición deberá tener un error menor o igual al 5%. El sentido de esta corriente es único, y circula desde los paneles al regulador solar.

**Nota:** Al utilizar transformadores de corriente para esta medición, deberá prestarse especial atención al sentido de sensado de los mismos, de forma tal de asegurar que la corriente de carga provista por los paneles fotovoltaicos sea medida como positiva.



#### 4.4.4 Tensión del banco de baterías

El datalogger deberá medir la tensión del banco de baterías. La tensión nominal del banco de baterías podrá ser de 12V, 24V y 48V. Sin embargo, durante los ciclos de carga, las tensiones a medir podrán ser superiores a las nominales. Debido a ello el datalogger deberá poder medir tensiones en el rango de 0 a 75V. La medición deberá tener un error menor o igual al 1%. La entrada deberá estar protegida por sobretensiones de hasta 80V, y no deberá consumir más de 10mA para el mayor valor de tensión. Deberá también, contar con un fusible de protección para evitar riesgos de incendio. Se recomienda el uso de un amplificador de instrumentación con alta impedancia de entrada para minimizar corrientes de fuga.

#### 4.4.5 Corriente de carga y descarga del banco de baterías

El datalogger deberá medir la corriente de carga y descarga del banco de baterías (si bien la corriente en cada caso es continua, el sentido de la misma es bidireccional). La corriente de carga es provista por el regulador solar al banco de baterías. La corriente de descarga es provista por el banco de baterías al inversor. El rango de valores que deberá poder medirse es de 0 a 300 A, en ambos sentidos. La medición deberá tener un error menor o igual al 5%.

**Nota:** Al utilizar transformadores de corriente para esta medición, deberá prestarse especial atención al sentido de sensado de los mismos, de forma tal de asegurar que la corriente de carga sea medidas como positiva, y la corriente de descarga como negativa.

#### 4.4.6 Corriente entregada por el cargador de baterías al banco de baterías.

El datalogger deberá medir la corriente continua de carga provista por el cargador de baterías al banco de baterías. El rango de valores que deberá poder medirse es de 0 a 300 A. Debido a que esta corriente puede ser del tipo pulsante, deberá medirse el valor "True-RMS" de la misma. La medición deberá tener un error menor o igual al 5%. El sentido de esta corriente es único, y circula desde el cargador de baterías al banco.

**Nota:** Al utilizar transformadores de corriente para esta medición, deberá prestarse especial atención al sentido de sensado de los mismos, de forma tal de asegurar que la corriente de carga sea medida como positiva.

#### 4.4.7 Temperatura del banco de baterías

El datalogger deberá contar con una entrada para sensores de temperatura NTC (de 10Kohms a 25°C). La tensión con la que se alimentará el sensor no deberá ser mayor o igual a 5V y no deberá superar los 24V. La corriente máxima admisible por el sensor a 25 C será de 0.25mA, de forma tal de evitar errores de medición por el auto-calentamiento del sensor. Deberá poder medirse una temperatura desde -15°C a 60°C.

#### 4.4.8 Tensión alterna de consumos de usuario

Las salidas de los inversores que se instalarán son del tipo senoidal pura. No obstante, debido a que en ciertos casos se instalará una llave selectora que permitirá conectar un grupo electrógeno como alimentación, el datalogger deberá medir el valor "True-RMS" de la tensión alterna entregada al usuario. El rango de tensiones a medir será de 0V a 300VAC, y no deberá consumir más de 10mA para el mayor valor de tensión. La medición deberá tener un error menor o igual al 5%. Deberá también, contar con un fusible de protección para evitar riesgos de incendio. Para garantizar la aislación galvánica entre el inversor y el datalogger, en esta medición se deberá utilizar un transformador de señal.

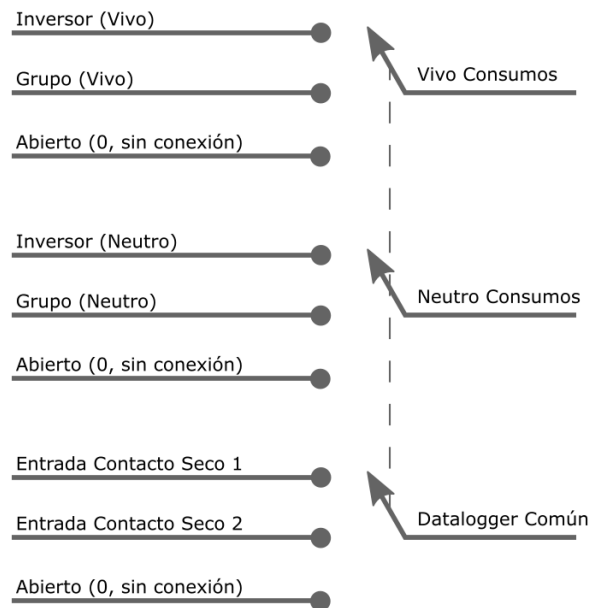
#### 4.4.9 Corriente alterna de consumos de usuario

De forma similar a la tensión entregada al usuario, deberá medirse el valor "True-RMS" de la corriente alterna de consumos del usuario. El rango a medir para esta variable es de 0A a 50A. La medición deberá tener un error menor o igual al 5%.

#### 4.4.10 Posición de la llave selectora

Como se explicó en la introducción, algunas de las instalaciones contarán con un grupo electrógeno para alimentar consumos de mayor potencia. Se instalará una llave selectora de tres puntos (trifásica) y tres posiciones (Inversor, Grupo y abierto, ó 0), para elegir alimentar los consumos desde el inversor o desde el grupo electrógeno (o no alimentarlos).

El datalogger deberá determinar la posición de la llave conectando las entradas de contacto seco al punto libre de la misma, según el esquema de conexión que se presenta a continuación:



De esta manera el datalogger podrá determinar la posición de la llave selectora leyendo los estados de las entradas de contacto seco.

**Importante:** las entradas de contacto seco deberán contar con filtros “anti-rebote” (ya sea implementados por Hardware o Software), para evitar el sensado incorrecto de los rebotes característicos de los interruptores mecánicos.

#### 4.5 Conectorización y cableado

La placa del datalogger deberá poseer las borneras necesarias para realizar la conexión de todos los sensores y cables que se utilizaran en el sistema. Dichas borneras deberán contar con la aislación de tensión necesaria entre bornes, así como también soportar las corrientes que circularán por los sensores.

**Importante:** Los cables que se utilizarán para conectar los sensores deberán ser mallados, de forma tal de minimizar el ruido electromagnético inducido en las mediciones. De esta forma, cada punto de medición deberá contar con una bornera extra para conectar la malla de cada cable a la “masa” del datalogger. El otro extremo de la malla del cable no deberá conectarse, para evitar formar “loops” susceptibles al ruido eléctrico generado por inducción magnética.

Las longitudes mínimas de los cables de los sensores a proveer se detallan en la tabla “Resumen de mediciones”.

Las borneras deberán ser del tipo “enchufables”, de forma tal de facilitar el conexionado de los cables y sus respectivas mallas a las mismas. A modo de ejemplo, las borneras deberán ser similares a las que se muestran a continuación:



#### 4.6 Resumen de mediciones

La siguiente tabla se presenta a modo de resumen de las mediciones antes explicadas:

Medición	Valores	Longitud mínima cables de sensores
Tensión paneles fotovoltaicos	0 - 160VCC. Error $\leq$ 1%. Protección por sobretensiones mayor a 200V. Consumo máximo 10mA.	4 m
Corriente paneles fotovoltaicos	0 - 300A. Error $\leq$ 5%. Unidireccional.	4 m
Tensión del banco de baterías	0 - 75VCC. Error $\leq$ 1%. Protección por sobretensiones mayor a 80V. Consumo máximo 10mA.	4 m
Corriente carga y descarga del banco de baterías	0 - 300A. Error $\leq$ 5%. Bidireccional.	4 m
Corriente del cargador de baterías	0 - 300A. Error $\leq$ 5%. Unidireccional. True RMS.	4 m
Temperatura del banco de baterías	-15°C a 60°C. Sensor NTC, corriente máxima a 25°C: 0.25mA. Alimentación 5V - 24V.	6 m
Tensión alterna de consumos de usuario	0 - 300VAC. Error $\leq$ 5%. True RMS. Consumo máximo 10mA. Aislación galvánica utilizando un transformador de señal.	3 m
Corriente alterna de consumos de usuario	0 - 50A. Error $\leq$ 5%. True RMS.	3 m
Posición de la llave selectora	Entradas de contacto seco. Corriente: 0.1mA - 1mA. Tensión máxima en las entradas: 5V.	3 m

## 5 Comunicación con el servidor

En esta sección se especificará el protocolo de comunicación entre las terminales datalogger y el servidor central.

### 5.1 Comunicación y envío de datos vía HTTP

El datalogger se comunicará con el servidor central a través de los comandos GET y POST de HTTP, utilizando un típico esquema "RESTful". El contenido de estos mensajes será transmitido en formato XML (texto). La única excepción a esto es la situación en el que el datalogger descargue una versión de firmware nueva desde el servidor. En este caso, el datalogger descargará el archivo de firmware en formato binario al enviar un comando GET HTTP a la URL especificada por el servidor.

En las secciones siguientes se especificará el esquema XML de cada mensaje, así como también las URLs y los parámetros para cada caso.

**Nota:** los esquemas XML de los comandos y reportes están disponibles en formato digital para ser solicitados por los fabricantes.

### 5.2 Secuencia de comunicación

La comunicación entre el datalogger y el servidor central es del estilo cliente-servidor: es decir, el datalogger siempre inicia la comunicación para pedir órdenes del servidor central y enviar datos al mismo. A su vez, el servidor responderá con comandos, ordenando al datalogger realizar los reportes que sean necesarios (pedidos de datos entre distintas fechas, cambios de configuración, etc.). El datalogger responderá a estos comandos y continuará "pidiendo órdenes" hasta que el servidor le indique al datalogger una nueva fecha y hora de reconexión para el envío de datos. El datalogger deberá entonces reconectarse a la fecha y hora programada (en el caso de que surgiera una alarma o evento, el datalogger deberá reportarla en forma inmediata, sin esperar a la nueva fecha de reporte).

El datalogger "pedirá órdenes" enviando el comando "check-in" al servidor, el cual deberá responder con alguna de las siguientes órdenes:

- Consulta de mediciones.
- Programación de fecha y hora de próxima conexión.
- Configuración de red.
- Configuración de mediciones.
- Configuración de alarmas.
- Configuración de eventos.
- Consulta de configuración de red.
- Consulta de configuración de mediciones.
- Consulta de configuración de alarmas.
- Consulta de configuración de eventos.
- Borrar memoria interna.
- Consulta de versión de firmware.
- Actualización de firmware.

En las siguientes secciones se detallará cada uno de estos comandos.

### 5.3 Formato de fecha y hora

El formato de la fecha y hora a utilizar en todos los reportes y comandos donde sea necesario será el siguiente:

**YYYY-MM-DDTHH:mm:ss**

Donde:

- **YYYY:** especifica el año de la fecha.
  - **MM:** especifica el mes de la fecha.
  - **DD:** especifica el día de la fecha.
  - **HH:** especifica la hora en formato 24hs.
  - **mm:** especifica los minutos.
  - **ss:** especifica los segundos
-

Ejemplo: 5 de septiembre de 2017, 15:05:17 horas se representa como: “**2017-09-05T15:05:17**”.

#### 5.4 Formato de hora

El formato de hora a utilizar en todos los reportes y comandos donde sea necesario será el siguiente:

**HH:mm:ss**

Donde:

- **HH**: especifica la hora en formato 24hs.
- **mm**: especifica los minutos.
- **ss**: especifica los segundos

Ejemplo: las 20:01:10 horas se representa como: “**20:01:10**”.

#### 5.5 Reportes enviados por el datalogger

El datalogger enviará al servidor central los reportes que se especificarán en las siguientes subsecciones.

En todos los reportes, el datalogger incluirá su identificación y contraseña como parámetros en la URL para autenticarse en el servidor central, siguiendo el siguiente formato:

**http://url\_servidor/nombre\_reporte\_o\_comando?ID=id&PASSWORD=password**

Donde:

- **Url\_Servidor**: es la URL del servidor, o la dirección IP del mismo.
- **Nombre\_reporte\_o\_comando**: es el nombre del reporte a enviar o comando a responder, y se indicará en cada caso.
- **id**: es el ID alfanumérico que se utiliza para identificar al datalogger.
- **password**: es el password alfanumérico que se utiliza para autenticar al datalogger.

##### 5.5.1 Check-in

El datalogger enviará el reporte de check-in a través de un GET HTTP a la siguiente url:

**http://url\_servidor/check\_in?ID=id&PASSWORD=password**

Como respuesta, el servidor enviará alguno de los comandos especificados en la sección 5.6. Este reporte será enviado por el datalogger por primera vez al encenderse y continuará siendo enviado hasta que el servidor le responda con el comando de programación de hora y fecha de próxima conexión (5.6.3).

##### 5.5.2 Pedido de sincronización de hora y fecha

El datalogger deberá mantener su reloj interno sincronizado con el del servidor central. Para ello, enviará periódicamente el pedido de la hora y fecha del servidor central, haciendo un GET HTTP a la siguiente url:

**http://url\_servidor/fecha\_y\_hora?ID=id&PASSWORD=password**

Como respuesta, el servidor enviará el comando especificado en la sección 5.6.2. El datalogger tomará los datos de fecha y hora recibidos y los utilizará para sincronizar su reloj interno.

##### 5.5.3 Reporte de mediciones

En el caso de que el servidor haya respondido al check-in con el comando de consulta de mediciones (5.6.1), el datalogger deberá responder haciendo un POST HTTP a la siguiente url:

**http://url\_servidor/mediciones?ID=id&PASSWORD=password**

El contenido del reporte deberá responder al siguiente esquema XML:

En este mensaje, los campos “**FechaYHoraComienzo**” y “**FechaYHoraFin**” especifican las fechas y horas de comienzo y de fin de los reportes respectivamente. Las mediciones serán enviadas en el

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="ReporteMediciones" nillable="true" type="ReporteMediciones" />
  <xs:complexType name="ReporteMediciones">
    <xs:sequence>
      <xs:element minOccurs="1" maxOccurs="1" name="FechaYHoraComienzo" type="xs:dateTime" />
      <xs:element minOccurs="1" maxOccurs="1" name="FechaYHoraFin" type="xs:dateTime" />
      <xs:element minOccurs="1" maxOccurs="1" name="Mediciones" type="ArrayOfString" />
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="ArrayOfString">
    <xs:sequence>
      <xs:element minOccurs="0" maxOccurs="unbounded" name="string" nillable="true" type="xs:string" />
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

arreglo de strings llamado “**Mediciones**”, y seguirán el formato descrito a continuación.

### 5.5.3.1 Formato de las mediciones

Cada renglón de mediciones incluirá los datos siguientes datos, separados por una coma (“,”) según el orden:

Posición	Medición
1	Fecha y hora de la medición.
2	Tensión de los paneles fotovoltaicos.
3	Corriente entregada por los paneles fotovoltaicos.
4	Potencia instantánea entregada por el regulador solar.
5	Energía diaria generada por los paneles fotovoltaicos.
6	Tensión del banco de baterías.
7	Corriente de carga y descarga del banco de baterías.
8	Estado de carga del banco de baterías.
9	Corriente entregada por el cargador de baterías al banco de baterías.
10	Temperatura del banco de baterías.
11	Tensión alterna de consumos de usuario.
12	Corriente alterna de consumos de usuario.
13	Potencia instantánea de CA.
14	Energía diaria consumida.
15	Posición de la llave selectora.

Se respetarán las unidades y precisiones especificadas en la sección 4.4.1.

Como convención, la corriente de carga de baterías tendrá signo positivo y la corriente de descarga de baterías tendrá signo negativo. El resto de las corrientes serán siempre positivas.

**Nota:** Se estima que guardando datos cada un minuto, cada día reportado por el datalogger al servidor central implicará una transmisión de 170kB de datos (esto sin contar los bytes de “overhead” a transmitir debido al protocolo TCP/IP)

El siguiente es un ejemplo de un reporte con tres mediciones durante el intervalo temporal especificado:

```
<?xml version="1.0" encoding="utf-8"?>
<ReporteMediciones>
  <FechaYHoraComienzo>2017-09-10T09:05:00</FechaYHoraComienzo>
  <FechaYHoraFin>2017-09-10T09:07:00</FechaYHoraFin>
  <Mediciones>
<string>2017-09-10T09:05:00,82.00,5.25,387.98,2354.58,54.35,5.10,3,0.00,26.5,218.59,1.05,229.52,982.51,1</string>
<string>2017-09-10T09:05:00,82.30,5.15,381.46,2361.05,54.45,5.03,3,0.00,26.5,218.19,1.15,250.92,986.33,1</string>
<string>2017-09-10T09:07:00,82.20,5.25,388.39,2367.41,54.47,5.01,3,0.00,26.6,218.29,1.07,233.57,990.51,1</string>
</Mediciones>
</ReporteMediciones>
```

#### 5.5.4 Reporte de alarmas

Cuando el datalogger detecte una o más alarmas (o posea alguna alarma guardada en su memoria interna sin reportar al servidor central), el mismo deberá haciendo un POST HTTP a la siguiente url:

[http://url\\_servidor/alarmas?ID=id&PASSWORD=password](http://url_servidor/alarmas?ID=id&PASSWORD=password)

El contenido del reporte deberá respetar el siguiente esquema XML:

En este mensaje, los campos “**FechaYHoraComienzo**” y “**FechaYHoraFin**” especifican las fechas y

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="ReporteAlarmas" nillable="true" type="ReporteAlarmas" />
  <xs:complexType name="ReporteAlarmas">
    <xs:sequence>
      <xs:element minOccurs="1" maxOccurs="1" name="FechaYHoraComienzo" type="xs:dateTime" />
      <xs:element minOccurs="1" maxOccurs="1" name="FechaYHoraFin" type="xs:dateTime" />
      <xs:element minOccurs="0" maxOccurs="1" name="Alarmas" type="ArrayOfString" />
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="ArrayOfString">
    <xs:sequence>
      <xs:element minOccurs="0" maxOccurs="unbounded" name="string" nillable="true" type="xs:string" />
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

horas de comienzo y de fin de los reportes respectivamente. Las alarmas serán enviadas en el arreglo de strings llamado “**Alarmas**”, y seguirán el siguiente formato:

[Fecha\_y\_hora],[CódigoDeAlarma],[ValorRegistrado],[AlarmaDisparada]

El campo “**AlarmaDisparada**” es un campo booleano, que indica si se entró en condición de alarma (true) o si se restableció la condición normal (false).

La siguiente tabla especifica el código de alarma y el valor a reportar con las mismas:

Alarma	Código	Valor a Reportar
Baja tensión en banco de baterías	100	Tensión del banco de baterías
Sobretensión en banco de baterías	101	Tensión del banco de baterías
Sobrecorriente de carga del regulador solar	102	Corriente del regulador solar
Sobrecorriente de carga del cargador de baterías	103	Corriente del cargador de baterías
Sobrecorriente de descarga del banco de baterías	104	Corriente del banco de baterías
Temperatura alta en el banco de baterías	105	Temperatura del banco de baterías
Temperatura baja en el banco de baterías	105	Temperatura del banco de baterías
Potencia nula diurna a la salida del regulador solar	200	Potencia a la salida del regulador solar
Potencia nula a la salida del inversor	300	Potencia a la salida del inversor
Sobrecorriente a la salida del inversor	301	Corriente a la salida del inversor

A modo de ejemplo, se incluye un mensaje XML válido para el reporte de alarmas:

```
<?xml version="1.0" encoding="utf-8"?>
<ReporteAlarmas>
  <FechaYHoraComienzo>2017-09-10T09:10:00</FechaYHoraComienzo>
  <FechaYHoraFin>2017-09-10T09:11:00</FechaYHoraFin>
  <Alarmas>
    <string>2017-09-10T09:10:41,200,5.2,true</string>
  </Alarmas>
</ReporteAlarmas>
```

### 5.5.5 Reporte de eventos

Cuando el datalogger detecte uno o más de los eventos definidos (o posea algún evento guardado en su memoria interna sin reportar al servidor central), el mismo deberá haciendo un POST HTTP a la siguiente url:

[http://url\\_servidor/eventos?ID=id&PASSWORD=password](http://url_servidor/eventos?ID=id&PASSWORD=password)

El contenido del reporte deberá responder al siguiente esquema XML:

En este mensaje, los campos “**FechaYHoraComienzo**” y “**FechaYHoraFin**” especifican las fechas y horas de comienzo y de fin de los reportes respectivamente. Los eventos serán enviados en el arreglo

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="ReporteEventos" nillable="true" type="ReporteEventos" />
  <xs:complexType name="ReporteEventos">
    <xs:sequence>
      <xs:element minOccurs="1" maxOccurs="1" name="FechaYHoraComienzo" type="xs:dateTime" />
      <xs:element minOccurs="1" maxOccurs="1" name="FechaYHoraFin" type="xs:dateTime" />
      <xs:element minOccurs="0" maxOccurs="1" name="Eventos" type="ArrayOfString" />
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="ArrayOfString">
    <xs:sequence>
      <xs:element minOccurs="0" maxOccurs="unbounded" name="string" nillable="true" type="xs:string" />
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

de strings llamado “**Eventos**”, y seguirán el siguiente formato:

[Fecha\_y\_hora],[CódigoDeEvento]

La siguiente tabla especifica el código de evento y el valor a reportar con las mismas:

Evento	Código
Encendido del sistema	100
Apagado del sistema	101
Reseteo del sistema por watchdog interno	102
Reseteo del sistema por watchdog externo	103
Reseteo del sistema a valores por defecto	104
Conexión a la red establecida	200
Pérdida de conexión con la red	201
Alarma de baja memoria disponible	300
Alarma de pérdida de datos por sobre-escritura	301

A modo de ejemplo, se incluye un mensaje XML válido para el reporte de eventos:

```
<?xml version="1.0" encoding="utf-8"?>
<ReporteEventos>
  <FechaYHoraComienzo>2017-09-10T09:20:00</FechaYHoraComienzo>
  <FechaYHoraFin>2017-09-10T09:21:00</FechaYHoraFin>
  <Eventos>
    <string>2017-09-10T09:20:15,200</string>
  </Eventos>
</ReporteEventos>
```



### 5.5.6 Reporte de Configuración de red

En el caso de que el servidor haya respondido al check-in con el comando de consulta de configuración de red (5.6.8), el datalogger deberá responder haciendo un POST HTTP a la siguiente url:

```
http://url_servidor/configuracion_red?ID=id&PASSWORD=password
```

El contenido del reporte deberá respetar el esquema de la sección 5.6.4.

### 5.5.7 Reporte de Configuración de mediciones

En el caso de que el servidor haya respondido al check-in con el comando de consulta de configuración de mediciones (5.6.9), el datalogger deberá responder haciendo un POST HTTP a la siguiente url:

```
http://url_servidor/configuracion_mediciones?ID=id&PASSWORD=password
```

El contenido del reporte deberá respetar el esquema de la sección 5.6.5.

### 5.5.8 Reporte de Configuración de alarmas

En el caso de que el servidor haya respondido al check-in con el comando de consulta de configuración de alarmas (5.6.10), el datalogger deberá responder haciendo un POST HTTP a la siguiente url:

```
http://url_servidor/configuracion_mediciones?ID=id&PASSWORD=password
```

El contenido del reporte deberá respetar el esquema de la sección 5.6.6.

### 5.5.9 Reporte de Configuración de eventos

En el caso de que el servidor haya respondido al check-in con el comando de consulta de configuración de eventos (5.6.11), el datalogger deberá responder haciendo un POST HTTP a la siguiente url:

```
http://url_servidor/configuracion_eventos?ID=id&PASSWORD=password
```

El contenido del reporte deberá respetar el esquema de la sección 5.6.7.

### 5.5.10 Reporte de versión de Firmware

En el caso de que el servidor haya respondido al check-in con el comando de consulta de versión de firmware (5.6.12), el datalogger deberá responder haciendo un POST HTTP a la siguiente url:

```
http://url_servidor/version_firmware?ID=id&PASSWORD=password
```

El contenido del reporte deberá seguir el siguiente esquema XML:

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="ReporteFirmware" nillable="true" type="ReporteFirmware" />
  <xs:complexType name="ReporteFirmware">
    <xs:sequence>
      <xs:element minOccurs="1" maxOccurs="1" name="VersionFirmware" type="xs:string" />
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

### 5.5.11 Reporte de borrado de memoria interna

En el caso de que el servidor haya respondido al check-in con el comando borrado de memoria interna (5.6.13), el datalogger deberá responder si la operación fue efectuada satisfactoriamente, haciendo un POST HTTP a la siguiente url:

```
http://url_servidor/borrado_memoria_interna?ID=id&PASSWORD=password
```

El contenido del reporte deberá seguir el siguiente esquema XML:

El valor “**MemoriaInternaBorrada**” será verdadero (“true”) si la operación fue ejecutada

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="ReporteBorradoMemoriaInterna" nillable="true" type="ReporteBorradoMemoriaInterna" />
  <xs:complexType name="ReporteBorradoMemoriaInterna">
    <xs:sequence>
      <xs:element minOccurs="1" maxOccurs="1" name="MemoriaInternaBorrada" type="xs:boolean" />
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

satisfactoriamente. Caso contrario, será falso (“false”).

#### 5.6 Comandos enviados por el servidor central

Como se explicó anteriormente, el servidor central responderá al reporte “check-in” (5.5.1) con alguno de los comandos que se explicarán a continuación. El datalogger seguirá haciendo “check-in” hasta que el servidor central envíe el comando de “Programación de fecha y hora de próxima conexión” (5.6.3).

### 5.6.1 Consulta de mediciones

Cuando el servidor central requiera obtener mediciones del datalogger, deberá responder respetando el siguiente esquema XML:

En esta respuesta, el servidor deberá indicar la fecha y hora de comienzo y de finalización de los

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="ConsultaMediciones" nillable="true" type="ConsultaMediciones" />
  <xs:complexType name="ConsultaMediciones">
    <xs:sequence>
      <xs:element minOccurs="1" maxOccurs="1" name="FechaYHoraComienzo" type="xs:dateTime" />
      <xs:element minOccurs="1" maxOccurs="1" name="FechaYHoraFin" type="xs:dateTime" />
      <xs:element minOccurs="1" maxOccurs="1" name="IntervaloReportes" type="IntervaloReportes" />
    </xs:sequence>
  </xs:complexType>
  <xs:simpleType name="IntervaloReportes">
    <xs:restriction base="xs:string">
      <xs:enumeration value="MINUTOS_1" />
      <xs:enumeration value="MINUTOS_5" />
      <xs:enumeration value="MINUTOS_15" />
      <xs:enumeration value="MINUTOS_30" />
      <xs:enumeration value="MINUTOS_60" />
    </xs:restriction>
  </xs:simpleType>
</xs:schema>
```

reportes requeridos, así como también el intervalo en minutos (1, 5, 15, 30 ó 60) entre las mediciones a reportar. Cuando este intervalo sea mayor al intervalo utilizado para guardar los registros de las mediciones en la memoria interna del datalogger, las mediciones reportadas se obtendrán seleccionando un subconjunto de las mediciones guardadas de forma tal de cumplir con el intervalo deseado (decimación). En el caso de que intervalo requerido sea menor al intervalo entre las mediciones guardadas en memoria, el datalogger responderá con la mayor cantidad de mediciones posibles obtenidas entre las fechas especificadas.

Mediante este mecanismo el servidor podrá controlar el tamaño (en bytes) de las mediciones a enviar por el datalogger, pudiendo seleccionar una menor cantidad de reportes para los dataloggers cuya conexión a internet no sea lo suficientemente veloz.

### 5.6.2 Sincronización de hora y fecha

Como respuesta al pedido de hora y fecha por parte del datalogger (sección 5.5.2), el servidor central responderá respetando el siguiente esquema XML:

El valor del campo "**FechaYHoraActual**" seguirá el formato especificado en la sección 5.3.

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="FechaYHora" nillable="true" type="FechaYHora" />
  <xs:complexType name="FechaYHora">
    <xs:sequence>
      <xs:element minOccurs="1" maxOccurs="1" name="FechaYHoraActual" type="xs:dateTime" />
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

### 5.6.3 Programación de fecha y hora de próxima conexión

El servidor central determinará la fecha y hora de la próxima conexión del datalogger respetando el siguiente esquema XML:

**Importante:** si la fecha y hora requerida por el servidor es incorrecta, o supera los 10 días de

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="ProximaConexion" nillable="true" type="ProximaConexion" />
  <xs:complexType name="ProximaConexion">
    <xs:sequence>
      <xs:element minOccurs="1" maxOccurs="1" name="HoraYFechaProximaConexion" type="xs:dateTime" />
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

diferencia con la fecha actual, el datalogger tomará por defecto que deberá conectarse nuevamente dentro de 24hs. De esta forma se evita que se pierda comunicación con las terminales por períodos prolongados de tiempo.

---

## 5.6.4 Configuración de red

El servidor central podrá realizar la configuración de los parámetros de red del datalogger al responder al reporte de “check-in” respetando el siguiente esquema XML:

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="ConfiguracionRed" nillable="true" type="ConfiguracionRed" />
  <xs:complexType name="ConfiguracionRed">
    <xs:sequence>
      <xs:element minOccurs="0" maxOccurs="1" name="TipoIpEthernet" nillable="true" type="TipoIP" />
      <xs:element minOccurs="0" maxOccurs="1" name="DataLoggerEthernetIP" type="xs:string" />
      <xs:element minOccurs="0" maxOccurs="1" name="PuertaDeEnlaceEthernetIP" type="xs:string" />
      <xs:element minOccurs="0" maxOccurs="1" name="MascaraSubRedEthernet" type="xs:string" />
      <xs:element minOccurs="0" maxOccurs="1" name="DNSPrimarioEthernet" type="xs:string" />
      <xs:element minOccurs="0" maxOccurs="1" name="DNSSecundarioEthernet" type="xs:string" />
      <xs:element minOccurs="0" maxOccurs="1" name="SsidWiFi" type="xs:string" />
      <xs:element minOccurs="0" maxOccurs="1" name="PasswordWiFi" type="xs:string" />
      <xs:element minOccurs="0" maxOccurs="1" name="SeguridadWiFi" nillable="true" type="TipoSeguridadWiFi" />
    />
    <xs:element minOccurs="0" maxOccurs="1" name="TipoIpWiFi" nillable="true" type="TipoIP" />
    <xs:element minOccurs="0" maxOccurs="1" name="DataLoggerWiFiIP" type="xs:string" />
    <xs:element minOccurs="0" maxOccurs="1" name="PuertaDeEnlaceWiFiIP" type="xs:string" />
    <xs:element minOccurs="0" maxOccurs="1" name="MascaraSubRedWiFi" type="xs:string" />
    <xs:element minOccurs="0" maxOccurs="1" name="DNSPrimarioWiFi" type="xs:string" />
    <xs:element minOccurs="0" maxOccurs="1" name="DNSSecundarioWiFi" type="xs:string" />
    <xs:element minOccurs="0" maxOccurs="1" name="URLServidorCentral" type="xs:string" />
    <xs:element minOccurs="0" maxOccurs="1" name="PuertoServidorCentral" type="xs:positiveInteger" />
    <xs:element minOccurs="0" maxOccurs="1" name="TimeoutConexion" type="xs:positiveInteger" />
    <xs:element minOccurs="0" maxOccurs="1" name="TimeoutInactividad" type="xs:positiveInteger" />
    <xs:element minOccurs="0" maxOccurs="1" name="IntentosReconexionPorCiclo" type="xs:positiveInteger" />
    <xs:element minOccurs="0" maxOccurs="1" name="EsperaReconexion" type="xs:positiveInteger" />
    <xs:element minOccurs="0" maxOccurs="1" name="EsperaRecomienzoCicloReconexion" type="xs:positiveInteger" />
  />
</xs:complexType>
</xs:element>
<xs:simpleType name="TipoIP">
  <xs:restriction base="xs:string">
    <xs:enumeration value="ESTATICA" />
    <xs:enumeration value="DHCP" />
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="TipoSeguridadWiFi">
  <xs:restriction base="xs:string">
    <xs:enumeration value="NINGUNA" />
    <xs:enumeration value="WEP" />
    <xs:enumeration value="WPA" />
    <xs:enumeration value="WPA2" />
  </xs:restriction>
</xs:simpleType>
</xs:schema>
```

### 5.6.5 Configuración de mediciones

El servidor central podrá realizar la configuración de las mediciones a realizar por el datalogger al responder al reporte de "check-in" respetando el siguiente esquema XML:

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="ConfiguracionMediciones" nillable="true" type="ConfiguracionMediciones" />
  <xs:complexType name="ConfiguracionMediciones">
    <xs:sequence>
      <xs:element minOccurs="1" maxOccurs="1" name="PeriodoMedicion" type="PeriodoMedicion" />
      <xs:element minOccurs="1" maxOccurs="1" name="BancoDeBaterias" type="TensionBancoDeBaterias" />
      <xs:element minOccurs="1" maxOccurs="1" name="TensionMaximaMuyBajo" type="xs:double" />
      <xs:element minOccurs="1" maxOccurs="1" name="TensionMaximaBajo" type="xs:double" />
      <xs:element minOccurs="1" maxOccurs="1" name="TensionMaximaMedio" type="xs:double" />
      <xs:element minOccurs="1" maxOccurs="1" name="TensionMaximaAlto" type="xs:double" />
      <xs:element minOccurs="1" maxOccurs="1" name="CoeficienteCorreccionTemperatura" type="xs:double" />
    </xs:sequence>
  </xs:complexType>
  <xs:simpleType name="PeriodoMedicion">
    <xs:restriction base="xs:string">
      <xs:enumeration value="MINUTOS_1" />
      <xs:enumeration value="MINUTOS_5" />
      <xs:enumeration value="MINUTOS_15" />
      <xs:enumeration value="MINUTOS_30" />
      <xs:enumeration value="MINUTOS_60" />
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="TensionBancoDeBaterias">
    <xs:restriction base="xs:string">
      <xs:enumeration value="BANCO12V" />
      <xs:enumeration value="BANCO24V" />
      <xs:enumeration value="BANCO48V" />
    </xs:restriction>
  </xs:simpleType>
</xs:schema>
```

### 5.6.6 Configuración de alarmas

El servidor central podrá realizar la configuración de las alarmas a reportar por el datalogger al responder al reporte de “check-in” respetando el siguiente esquema XML:

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="ConfiguracionAlarmas" nillable="true" type="ConfiguracionAlarmas" />
  <xs:complexType name="ConfiguracionAlarmas">
    <xs:sequence>
      <xs:element minOccurs="1" maxOccurs="1" name="TensionBajaBateria" type="positiveDecimal" />
      <xs:element minOccurs="1" maxOccurs="1" name="TiempoAlarmaBajaBateria" type="xs:positiveInteger" />
      <xs:element minOccurs="1" maxOccurs="1" name="TensionRestablecimientoBajaBateria" type="positiveDecimal" />
      <xs:element minOccurs="1" maxOccurs="1" name="TiempoRestablecimientoAlarmaBajaBateria"
type="xs:positiveInteger" />
      <xs:element minOccurs="1" maxOccurs="1" name="AlarmaBajaBateriaHabilitada" type="xs:boolean" />
      <xs:element minOccurs="1" maxOccurs="1" name="SobreTensionBateria" type="positiveDecimal" />
      <xs:element minOccurs="1" maxOccurs="1" name="TiempoAlarmaSobreTensionBateria" type="xs:positiveInteger" />
      <xs:element minOccurs="1" maxOccurs="1" name="TensionRestablecimientoSobreTensionBateria"
type="positiveDecimal" />
      <xs:element minOccurs="1" maxOccurs="1" name="TiempoRestablecimientoAlarmaSobreTensionBateria"
type="xs:positiveInteger" />
      <xs:element minOccurs="1" maxOccurs="1" name="AlarmaSobreTensionBateriaHabilitada" type="xs:boolean" />
      <xs:element minOccurs="1" maxOccurs="1" name="SobreCorrienteSolarBateria" type="positiveDecimal" />
      <xs:element minOccurs="1" maxOccurs="1" name="TiempoAlarmaSobreCorrienteSolarBateria"
type="xs:positiveInteger" />
      <xs:element minOccurs="1" maxOccurs="1" name="CorrienteSolarRestablecimientoSobreCorrienteBateria"
type="positiveDecimal" />
      <xs:element minOccurs="1" maxOccurs="1" name="TiempoRestablecimientoAlarmaSobreCorrienteSolarBateria"
type="xs:positiveInteger" />
      <xs:element minOccurs="1" maxOccurs="1" name="AlarmaSobreCorrienteSolarHabilitada" type="xs:boolean" />
      <xs:element minOccurs="1" maxOccurs="1" name="SobreCorrienteCargadorBateria" type="positiveDecimal" />
      <xs:element minOccurs="1" maxOccurs="1" name="TiempoAlarmaSobreCorrienteCargadorBateria"
type="xs:positiveInteger" />
      <xs:element minOccurs="1" maxOccurs="1" name="CorrienteCargadorRestablecimientoSobreCorrienteBateria"
type="positiveDecimal" />
      <xs:element minOccurs="1" maxOccurs="1" name="TiempoRestablecimientoAlarmaSobreCorrienteCargadorBateria"
type="xs:positiveInteger" />
      <xs:element minOccurs="1" maxOccurs="1" name="AlarmaSobreCorrienteCargadorHabilitada" type="xs:boolean" />
      <xs:element minOccurs="1" maxOccurs="1" name="SobreCorrienteoDescargaBateria" type="positiveDecimal" />
      <xs:element minOccurs="1" maxOccurs="1" name="TiempoAlarmaSobreCorrienteDescargaBateria"
type="xs:positiveInteger" />
      <xs:element minOccurs="1" maxOccurs="1"
name="CorrienteDescargaRestablecimientoSobreCorrienteDescargaBateria" type="positiveDecimal" />
      <xs:element minOccurs="1" maxOccurs="1" name="TiempoRestablecimientoAlarmaSobreCorrienteDescargaBateria"
type="xs:positiveInteger" />
      <xs:element minOccurs="1" maxOccurs="1" name="AlarmaSobreCorrienteDescargaHabilitada" type="xs:boolean" />
      <xs:element minOccurs="1" maxOccurs="1" name="PotenciaDiurnaMinimaReguladorSolar" type="positiveDecimal" />
      <xs:element minOccurs="1" maxOccurs="1" name="TiempoAlarmaPotenciaDiurnaMinimaReguladorSolar"
type="xs:positiveInteger" />
      <xs:element minOccurs="1" maxOccurs="1" name="PotenciaRestablecimientoAlarmaPotenciaDiurnaNula"
type="positiveDecimal" />
      <xs:element minOccurs="1" maxOccurs="1" name="TiempoRestablecimientoAlarmaPotenciaDiurnaNula"
type="xs:positiveInteger" />
      <xs:element minOccurs="1" maxOccurs="1" name="ComienzoHorarioDurno" type="xs:time" />
      <xs:element minOccurs="1" maxOccurs="1" name="FinalizacionHorarioDurno" type="xs:time" />
      <xs:element minOccurs="1" maxOccurs="1" name="AlarmaPotenciaDiurnaNulaHabilitada" type="xs:boolean" />
      <xs:element minOccurs="1" maxOccurs="1" name="PotenciaMinimaInversor" type="positiveDecimal" />
      <xs:element minOccurs="1" maxOccurs="1" name="TiempoAlarmaPotenciaMinimaInversor" type="xs:positiveInteger" />
    />
    <xs:element minOccurs="1" maxOccurs="1" name="PotenciaRestablecimientoAlarmaPotenciaNulaInversor"
type="positiveDecimal" />
    <xs:element minOccurs="1" maxOccurs="1" name="TiempoRestablecimientoAlarmaPotenciaNulaInversor"
type="xs:positiveInteger" />
    <xs:element minOccurs="1" maxOccurs="1" name="AlarmaPotenciaNulaInversorHabilitada" type="xs:boolean" />
    <xs:element minOccurs="1" maxOccurs="1" name="SobreCorrienteInversor" type="positiveDecimal" />
    <xs:element minOccurs="1" maxOccurs="1" name="TiempoAlarmaSobreCorrienteInversor" type="xs:positiveInteger" />
  />
  <xs:element minOccurs="1" maxOccurs="1" name="CorrienteRestablecimientoAlarmaSobreCorrienteInversor"
type="positiveDecimal" />
  <xs:element minOccurs="1" maxOccurs="1" name="TiempoRestablecimientoAlarmaSobreCorrienteInversor"
type="xs:positiveInteger" />
  <xs:element minOccurs="1" maxOccurs="1" name="AlarmaSobreCorrienteInversorHabilitada" type="xs:boolean" />

```

```

    <xs:element minOccurs="1" maxOccurs="1" name="TemperaturaMaximaBaterias" type="positiveDecimal" />
    <xs:element minOccurs="1" maxOccurs="1" name="TiempoAlarmaTemperaturaAltaBaterias"
type="xs:positiveInteger" />
    <xs:element minOccurs="1" maxOccurs="1" name="TemperaturaRestablecimientoAlarmaTemperaturaAltaBaterias"
type="positiveDecimal" />
    <xs:element minOccurs="1" maxOccurs="1" name="TiempoRestablecimientoAlarmaTemperaturaAltaBaterias"
type="xs:positiveInteger" />
    <xs:element minOccurs="1" maxOccurs="1" name="AlarmaTemperaturaAltaBateriasHabilitada"
type="xs:boolean" />
    <xs:element minOccurs="1" maxOccurs="1" name="TemperaturaMinimaBaterias" type="xs:double" />
    <xs:element minOccurs="1" maxOccurs="1" name="TiempoAlarmaTemperaturaBajaBaterias"
type="xs:positiveInteger" />
    <xs:element minOccurs="1" maxOccurs="1" name="TemperaturaRestablecimientoAlarmaTemperaturaBajaBaterias"
type="xs:double" />
    <xs:element minOccurs="1" maxOccurs="1" name="TiempoRestablecimientoAlarmaTemperaturaBajaBaterias"
type="xs:positiveInteger" />
    <xs:element minOccurs="1" maxOccurs="1" name="AlarmaTemperaturaBajaBateriasHabilitada"
type="xs:boolean" />
  </xs:sequence>
</xs:complexType>
<xs:simpleType name="positiveDecimal">
  <xs:restriction base="xs:decimal">
    <xs:minInclusive value="0"/>
  </xs:restriction>
</xs:simpleType>
</xs:schema>

```



### 5.6.7 Configuración de eventos

El servidor central podrá realizar la configuración de los eventos a reportar por el datalogger al responder al reporte de “check-in” respetando el siguiente esquema XML:

### 5.6.8 Consulta de configuración de red

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="ConfiguracionEventos" nillable="true" type="ConfiguracionEventos" />
  <xs:complexType name="ConfiguracionEventos">
    <xs:sequence>
      <xs:element minOccurs="1" maxOccurs="1" name="ReporteEncendidoHabilitado" type="xs:boolean" />
      <xs:element minOccurs="1" maxOccurs="1" name="ReporteReseteoWatchdogInternoHabilitado" type="xs:boolean" />
      <xs:element minOccurs="1" maxOccurs="1" name="ReporteReseteoWatchdogExternoHabilitado" type="xs:boolean" />
      <xs:element minOccurs="1" maxOccurs="1" name="ReporteReseteoValoresPorDefectoHabilitado" type="xs:boolean" />
    />
    <xs:element minOccurs="1" maxOccurs="1" name="ReporteConexionRedHabilitado" type="xs:boolean" />
    <xs:element minOccurs="1" maxOccurs="1" name="ReporteDesconexionRedHabilitado" type="xs:boolean" />
    <xs:element minOccurs="1" maxOccurs="1" name="EspacioLibreMinimoMemoria" type="xs:positiveInteger" />
    <xs:element minOccurs="1" maxOccurs="1" name="ReporteBajoEspacioLibreMemoriaHabilitado" type="xs:boolean" />
    <xs:element minOccurs="1" maxOccurs="1" name="ReportePerdidaDeDatosHabilitado" type="xs:boolean" />
  </xs:sequence>
</xs:complexType>
```

El servidor central podrá consultar la configuración de los parámetros de red del datalogger al responder al reporte de “check-in” respetando el siguiente esquema XML:

El datalogger deberá responder con los datos configurados en el mismo, según el reporte de la

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="ConsultaConfiguracionRed" nillable="true" type="ConsultaConfiguracionRed" />
  <xs:complexType name="ConsultaConfiguracionRed" />
</xs:schema>
```

sección 5.6.4.

### 5.6.9 Consulta de configuración de mediciones

El servidor central podrá consultar la configuración de las mediciones a realizar por el datalogger al responder al reporte de “check-in” respetando el siguiente esquema XML:

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="ConsultaConfiguracionMediciones" nillable="true" type="ConsultaConfiguracionMediciones" />
  <xs:complexType name="ConsultaConfiguracionMediciones" />
</xs:schema>
```

El datalogger deberá responder con los datos configurados en el mismo, según el reporte de la sección 5.5.7.

### 5.6.10 Consulta de configuración de alarmas

El servidor central podrá consultar la configuración de las alarmas a reportar por el datalogger al responder al reporte de “check-in” respetando el siguiente esquema XML:

El datalogger deberá responder con los datos configurados en el mismo, según el reporte de la

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="ConsultaConfiguracionAlarmas" nillable="true" type="ConsultaConfiguracionAlarmas" />
  <xs:complexType name="ConsultaConfiguracionAlarmas" />
</xs:schema>
```

sección 5.5.8.

### 5.6.11 Consulta de configuración de eventos

El servidor central podrá consultar la configuración de los eventos a reportar por el datalogger al responder al reporte de “check-in” respetando el siguiente esquema XML:

El datalogger deberá responder con los datos configurados en el mismo, según el reporte de la sección 5.5.9.

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="ConsultaConfiguracionEventos" nillable="true" type="ConsultaConfiguracionEventos" />
  <xs:complexType name="ConsultaConfiguracionEventos" />
</xs:schema>
```

### 5.6.12 Consulta de versión de Firmware

El servidor central podrá consultar la versión del firmware del datalogger al responder al reporte de “check-in” respetando el siguiente esquema XML:

El datalogger deberá responder con los datos configurados en el mismo, según el reporte de la

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="ConsultaVersionFirmware" nillable="true" type="ConsultaVersionFirmware" />
  <xs:complexType name="ConsultaVersionFirmware" />
</xs:schema>
```

sección 5.5.10.

### 5.6.13 Borrar memoria interna

El servidor central podrá indicar al datalogger que debe borrar los datos medidos de su memoria interna al responder al reporte de “check-in” respetando el siguiente esquema XML:

El datalogger deberá responder con el resultado de la operación, según el reporte de la sección 5.5.11.

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="BorrarMemoriaInterna" nillable="true" type="BorrarMemoriaInterna" />
  <xs:complexType name="BorrarMemoriaInterna" />
</xs:schema>
```

### 5.6.14 Actualización de Firmware

El servidor central podrá indicar que el datalogger debe actualizar su firmware al responder al reporte de “check-in” respetando el siguiente esquema XML:

La URL indicada apuntará al archivo con el nuevo firmware del datalogger, el cual deberá ser

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="ActualizarFirmware" nillable="true" type="ActualizarFirmware" />
  <xs:complexType name="ActualizarFirmware">
    <xs:sequence>
      <xs:element minOccurs="1" maxOccurs="1" name="URLFirmware" type="xs:anyURI" />
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

descargado (utilizando un GET HTTP), verificado en su integridad (CRC) y utilizado por el datalogger para realizar la actualización.

### 5.6.15 Error de autenticación o comando incorrecto

En caso de que la información de autenticación (ID y password) o el reporte realizado por el datalogger sea incorrecto, el servidor central deberá responder respetando el siguiente esquema XML:

El campo **"Error"** especificará el tipo de error y estará acompañado por el campo **"MensajeError"**,

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="ErrorReporte" nillable="true" type="ErrorReporte" />
  <xs:complexType name="ErrorReporte">
    <xs:sequence>
      <xs:element minOccurs="1" maxOccurs="1" name="Error" type="errorTipo" />
      <xs:element minOccurs="1" maxOccurs="1" name="MensajeError" type="xs:string" />
    </xs:sequence>
  </xs:complexType>
  <xs:simpleType name="errorTipo">
    <xs:restriction base="xs:string">
      <xs:enumeration value="ERROR_AUTENTICACION" />
      <xs:enumeration value="ERROR_URL" />
      <xs:enumeration value="ERROR_PARAMETROS" />
    </xs:restriction>
  </xs:simpleType>
</xs:schema>
```

el cual contendrá una descripción del error en formato texto.

## **6 Documentación**

Junto al datalogger, deberán entregarse un manual de instalación y un manual de usuario.

### **6.1 Manual de Instalación**

El manual de instalación deberá explicar el procedimiento de instalación y puesta en funcionamiento del datalogger en el sistema para el que fue diseñado. Estará dirigido a los instaladores del sistema, los cuales normalmente contarán con conocimientos técnicos.

Deberá incluir una hoja de especificaciones técnicas, un diagrama típico de conexión y cableado y una descripción del funcionamiento del datalogger, explicando el uso de los pulsadores e indicadores luminosos.

Asimismo, deberán explicarse el procedimiento de configuración de las interfaces de red (Wi-Fi y Ethernet) y el procedimiento de verificación de correcta instalación, funcionamiento y comunicación con el servidor central.

El manual deberá contar con una sección de resolución de problemas típicos y un procedimiento de diagnóstico de fallas para facilitar la tarea de los instaladores del sistema.

### **6.2 Manual de usuario**

Este manual será el que utilizará el usuario final del sistema y explicará el funcionamiento del datalogger en términos generales. Deberá estar dirigido al público en general (es decir a personas sin formación técnica), por lo que deberá estar redactado con términos sencillos y de fácil entendimiento. Deberá incluir procedimientos para el encendido, apagado, reseteo y diagnóstico del estado del sistema (funcionamiento, conectividad, etc.) utilizando los indicadores luminosos del datalogger.

### **6.3 Garantía**

El oferente deberá garantizar por defectos de fabricación por el término de dos (2) años a partir de la fecha de entrega.

La reposición de cualquiera de los elementos por falla de fabricación o prestaciones respecto de los valores garantizados deberá hacerse en pesos argentinos.

Todas las garantías mencionadas deberán ser suministradas al contratante.

En caso de productos que no sean fabricados en el país del contratante se exige la designación de un representante local para reclamos en garantía.

### **6.4 Seguridad eléctrica**

Los datalogger deberán poseer la Certificación de Seguridad según Resolución 508/2015 de la Secretaría de Industria, Comercio y Minería de la Nación.

---

## 2- Desarrollo del Software

### 7 Introducción

En la presente sección se detallan los requerimientos funcionales y técnicos del servidor central de prueba que se utilizará para testear la comunicación y la funcionalidad de los sistemas de monitoreo (dataloggers) a instalar en los sistemas de generación fotovoltaica del PERMER.

La función de los dataloggers es la de medir el valor de múltiples variables de interés (tensiones, corrientes y temperaturas) en función del tiempo (hora y fecha), filtrarlas, analizarlas y almacenarlas. Dichas mediciones y otros datos (alarmas y eventos) serán enviados vía internet (TCP/IP) a un servidor central, utilizando el protocolo especificado en el documento de especificaciones técnicas del datalogger (“Especificaciones Equipo Datalogger”).

En primera instancia se desarrollará un servidor central de prueba, de forma tal que el mismo permita validar el correcto funcionamiento de los dataloggers a utilizar. Este servidor contará con las funcionalidades básicas necesarias para el almacenamiento, procesado, filtrado y presentación de los datos obtenidos de hasta 500 terminales.

El servidor contará con una base de datos relacional, en la cual se almacenarán los datos reportados por los dataloggers, así como también las distintas entidades necesarias para el funcionamiento del sistema (cuentas de usuarios, información sobre las escuelas donde se instalarán los dataloggers, etc.).

De forma tal de facilitar la instalación y prueba del servidor (deployment) se entregará una imagen de un disco de una máquina virtual, el cual contendrá pre-instalados todos los requerimientos de software (servidor web, motor de base de datos, configuración de red, etc.) necesarios para el funcionamiento del servidor de prueba.

**Importante:** Este desarrollo inicial servirá como base para el desarrollo del servidor central que finalmente será utilizado en producción para la recolección de los datos de todos los dataloggers a instalar (pudiendo llegar a contar hasta más de 2000 terminales). Por esta razón es de vital importancia que el proceso de diseño y desarrollo del servidor de prueba contemple la posibilidad de escalar (tanto a nivel software como a nivel de infraestructura de hardware), sin que sea necesario un proceso de rediseño completo.

---

## 8 Descripción Funcional

En esta sección se especificarán las funcionalidades que el servidor central de prueba deberá proveer.

### 8.1 Comunicación con las terminales (dataloggers)

El esquema de comunicación con los dataloggers será del estilo cliente-servidor: el servidor central esperará en el puerto 80 (http) las conexiones entrantes provenientes de los dataloggers; esto significa que el proceso de comunicación (apertura de sockets) siempre será iniciado por los dataloggers, ya que los mismos conocen la dirección IP o URL del servidor central (el servidor central no conocerá, a priori, las direcciones IP de los dataloggers).

Los dataloggers obtendrán “órdenes” del servidor central al conectarse periódicamente con el mismo, utilizando el protocolo de comunicación especificado en el documento de especificaciones técnicas del datalogger (“Especificaciones Equipo Datalogger”).

El servidor deberá generar y enviar las órdenes necesarias a cada datalogger, ya sea en forma automática o bajo requerimiento del usuario.

### 8.2 Órdenes del servidor generadas en forma automática

Las órdenes enviadas en forma automática son las siguientes:

- **Consulta de mediciones:** El servidor pedirá periódicamente las mediciones que el datalogger haya recopilado desde su último reporte.

**Importante:** de forma tal de no sobrecargar al servidor con demasiadas conexiones simultáneas, el servidor deberá programar o agendar los pedidos de mediciones en horarios repartidos homogéneamente en el tiempo.

- **Sincronización de fecha y hora:** El servidor sincronizará la hora y fecha con los dataloggers al menos una vez por semana. Esta orden también podrá ser requerida en forma manual por el usuario.
- **Programación de hora y fecha de próxima conexión:** Al haber recibido los datos de las mediciones del datalogger, y si no tuviera otra orden pendiente de enviar, el servidor central indicará el datalogger la hora y fecha en la que deberá realizar la próxima conexión en forma automática. Dicha fecha podrá ser modificada en forma manual por el usuario.
- **Configuración de red:** En el caso de que el usuario haya realizado algún cambio en la configuración de red de un datalogger en particular, el servidor enviará esta orden en forma automática cuando dicho datalogger realice su próxima conexión con el sistema.
- **Configuración de mediciones:** En el caso de que el usuario haya realizado algún cambio en la configuración de mediciones de un datalogger en particular, el servidor enviará esta orden en forma automática cuando dicho datalogger realice su próxima conexión con el sistema.
- **Configuración de alarmas:** En el caso de que el usuario haya realizado algún cambio en la configuración de alarmas de un datalogger en particular, el servidor enviará esta orden en forma automática cuando dicho datalogger realice su próxima conexión con el sistema.
- **Configuración de eventos:** En el caso de que el usuario haya realizado algún cambio en la configuración de eventos de un datalogger en particular, el servidor enviará esta orden en forma automática cuando dicho datalogger realice su próxima conexión con el sistema.
- **Error en la autenticación o comando incorrecto:** Cuando el sistema detecte un envío de credenciales incorrecto por parte de un datalogger, o una URL de reporte incorrecta, el mismo enviará una respuesta especificando el error, en concordancia con el protocolo especificado en el documento “Especificaciones Equipo Datalogger”.

### 8.3 Órdenes del servidor generadas manualmente por el usuario

- **Consulta de configuración de red:** Cuando el usuario así lo requiera, el servidor generará la orden de consulta de configuración de red de un datalogger en particular. Esta orden será luego enviada cuando dicho datalogger realice su próxima conexión con el sistema. La base de datos del sistema se actualizará automáticamente para reflejar los datos recibidos.

- **Consulta de configuración de mediciones:** Cuando el usuario así lo requiera, el servidor generará la orden de consulta de configuración de mediciones de un datalogger en particular. Esta orden será luego enviada cuando dicho datalogger realice su próxima conexión con el sistema. La base de datos del sistema se actualizará automáticamente para reflejar los datos recibidos.
- **Consulta de configuración de alarmas:** Cuando el usuario así lo requiera, el servidor generará la orden de consulta de configuración de alarmas de un datalogger en particular. Esta orden será luego enviada cuando dicho datalogger realice su próxima conexión con el sistema. La base de datos del sistema se actualizará automáticamente para reflejar los datos recibidos.
- **Consulta de configuración de eventos:** Cuando el usuario así lo requiera, el servidor generará la orden de consulta de configuración de eventos de un datalogger en particular. Esta orden será luego enviada cuando dicho datalogger realice su próxima conexión con el sistema. La base de datos del sistema se actualizará automáticamente para reflejar los datos recibidos.
- **Consulta de versión de firmware:** Cuando el usuario así lo requiera, el servidor generará la orden de consulta de versión de firmware de un datalogger en particular. Esta orden será luego enviada cuando dicho datalogger realice su próxima conexión con el sistema. La base de datos del sistema se actualizará automáticamente para reflejar los datos recibidos.
- **Orden de borrado de memoria interna:** Cuando el usuario así lo requiera, el servidor generará la orden de borrado de memoria interna de un datalogger en particular. Esta orden será luego enviada cuando dicho datalogger realice su próxima conexión con el sistema.
- **Actualización de versión de firmware:** Cuando el usuario así lo requiera, el servidor generará la orden de actualización de versión de firmware de un datalogger en particular. Esta orden será luego enviada cuando dicho datalogger realice su próxima conexión con el sistema. Al completarse el proceso de actualización satisfactoriamente, la versión de firmware registrada en la base de datos del sistema se actualizará automáticamente.

#### 8.4 Entidades

El servidor central deberá proveer una interfaz amigable para el alta, la baja y las modificaciones (ABM) de las distintas entidades que serán parte del sistema.

**Nota:** Para realizar las bajas de las entidades se recomienda utilizar una baja “lógica” para evitar problemas de consistencia en las relaciones entre las entidades.

Por “entidad” se entenderán los distintos objetos del sistema de los cuales se modelarán y almacenarán información en la base de datos. Cada entidad tendrá propiedades, las cuales deberán ser validadas por el sistema a la hora de ser ingresadas o modificadas (por ejemplo, el DNI de un usuario deberá ser un valor numérico entero positivo, etc.). Asimismo, las entidades poseerán relaciones de distintos tipos, las cuales serán especificadas en cada caso.

Las entidades que como **mínimo** deberá proveer el sistema serán:

- Usuario del Sistema
  - Escuela
  - Datalogger
  - Configuración de Red
  - Configuración de Mediciones
  - Configuración de Alarmas
  - Configuración de Eventos
  - Medición
  - Alarma
  - Evento
  - Firmware
-

**Importante:** El esquema de la base de datos relacional deberá ser generado automáticamente por el servidor. Es decir, no deberá ser necesario ejecutar un script para configurar el esquema de la base de datos por primera vez (o al haber modificaciones de entidades o relaciones), sino que el sistema deberá encargarse de dicha tarea automáticamente.

#### 8.4.1 Entidad: Usuario del Sistema

Esta entidad representará un usuario del sistema. El servidor deberá proveer una página de ABM para esta entidad, la cual validará que los datos ingresados sean correctos. Deberá también permitir la duplicación de una entidad para generar una nueva sin que sea necesario ingresar todos los datos nuevamente.

Como mínimo deberá contener las siguientes propiedades:

- **Id de la entidad:** Primary Key. Número utilizado para identificar unívocamente a la entidad. Autogenerado por el sistema y no modificable.
- **Nombre y Apellido:** Tipo string, longitud máxima 80 caracteres. No se aceptarán repeticiones.
- **DNI:** Valor numérico entero positivo. No se aceptarán repeticiones.
- **E-mail:** Email con formato válido del usuario del sistema.
- **Tipo de usuario:** Tipo de usuario que indica sus permisos. Referirse a la sección 8.5.
- **Comentarios:** Tipo string, longitud máxima 255 caracteres.

#### 8.4.2 Entidad: Escuela

Estas entidades representarán a las escuelas que forman parte del proyecto de monitoreo de instalaciones fotovoltaicas. El servidor deberá proveer una página de ABM para esta entidad, la cual validará que los datos ingresados sean correctos. Deberá también permitir la duplicación de una entidad para generar una nueva sin que sea necesario ingresar todos los datos nuevamente.

Como mínimo deberá contener las siguientes propiedades:

- **Id de la entidad:** Primary Key. Número utilizado para identificar unívocamente la entidad. Autogenerado por el sistema y no modificable.
- **Nombre de la escuela:** Tipo string, longitud máxima 80 caracteres. No se aceptarán repeticiones.
- **Provincia:** Campo seleccionable de las 23 provincias argentinas.
- **Dirección:** Dirección de la escuela. Tipo string, longitud máxima 80 caracteres.
- **Latitud y Longitud:** Tipo string, longitud máxima 25 caracteres.
- **Nombre de contacto:** Tipo string, longitud máxima 80 caracteres.
- **Teléfono de contacto:** Tipo string, longitud máxima 20 caracteres.
- **E-mail:** Email de contacto de la escuela con formato válido.
- **Comentarios:** Tipo string, longitud máxima 255 caracteres.

##### 8.4.2.1 Relaciones con otras Entidades

A cada entidad "Escuela" se le podrá asignar uno o más de las entidades "Datalogger"; esto representará que en cada escuela podrá haber uno o más dataloggers instalados. Sin embargo, cada "Datalogger" estará asignado a una única escuela.

#### 8.4.3 Entidad: Datalogger

Estas entidades representarán a los dataloggers que forman parte del proyecto de monitoreo de instalaciones fotovoltaicas. El servidor deberá proveer una página de ABM para esta entidad, la cual validará que los datos ingresados sean correctos.

Como mínimo deberá contener las siguientes propiedades:

- **Id de la entidad:** Primary Key. Número utilizado para identificar unívocamente la entidad. Autogenerado por el sistema y no modificable.
  - **ID del datalogger:** ID que utilizará el datalogger para identificarse con el servidor. Tipo string alfanumérico, longitud máxima 25 caracteres.
  - **Contraseña:** Contraseña que utilizará el datalogger para autenticarse con el servidor. Tipo string alfanumérico, longitud máxima 25 caracteres.
-



- **Fecha de último contacto:** Campo del tipo “DATETIME” o “TIMESTAMP”, que registrará la última fecha de comunicación con el equipo, según formato “YYYY-MM-DDTHH:mm:ss”.
- **Nivel de loggeo:** Tipo numérico entero. Indicará el nivel de loggeo de las comunicaciones, advertencias, errores y demás mensajes recibidos del datalogger, según la convención: “0=sin loggeo, 1=loggeo errores, 2=loggeo errores y advertencias, 3=loggeo completo”. Referirse a la sección 8.10 para más información.
- **Comentarios:** Tipo string, longitud máxima 255 caracteres.

**Nota:** Se deberá mostrar la versión de firmware que el datalogger tiene instalada. Referirse a la sección 8.9 para más información.

#### 8.4.3.1 Relaciones con otras Entidades

Cada entidad “Datalogger” deberá estar asignado a una única entidad “Escuela”. Es decir, dos o más escuelas no podrán compartir el mismo datalogger. Sin embargo, una “Escuela” podrá tener asignados más de un “Datalogger”.

Cada entidad “Datalogger” deberá tener asignada una única configuración de red (entidad “Configuración de Red”) y viceversa.

Cada entidad “Datalogger” deberá tener asignada una única configuración de mediciones (entidad “Configuración de Mediciones”) y viceversa.

Cada entidad “Datalogger” deberá tener asignada una única configuración de alarmas (entidad “Configuración de Alarmas”) y viceversa.

Cada entidad “Datalogger” deberá tener asignada una única configuración de eventos (entidad “Configuración de Eventos”) y viceversa.

Cada entidad “Datalogger” deberá tener asignado un único Firmware (entidad “Firmware”).

Cada entidad “Datalogger” podrá tener asignada 0 o más reportes de mediciones (entidad “Medición”).

Cada entidad “Datalogger” podrá tener asignada 0 o más reportes de alarmas (entidad “Alarma”).

Cada entidad “Datalogger” podrá tener asignada 0 o más reportes de evento (entidad “Evento”).

#### 8.4.4 Entidad: Configuración de Red

Estas entidades representarán la configuración de red de las interfaces Ethernet y Wi-Fi de los dataloggers. El servidor deberá proveer una página de ABM para esta entidad, la cual validará que los datos ingresados sean correctos. Deberá también permitir la duplicación de una entidad para generar una nueva sin que sea necesario ingresar todos los datos nuevamente.

Como mínimo deberá contener las siguientes propiedades:

- **Id de la entidad:** Primary Key. Número utilizado para identificar unívocamente la entidad. Autogenerado por el sistema y no modificable.
  - **Ciente DHCP Interfaz Ethernet Habilitado:** Campo booleano que indicará si la interfaz Ethernet del datalogger obtendrá una dirección IP y configuración de red en forma dinámica (verdadero) o utilizará la dirección IP estática configurada (falso). Por defecto estará deshabilitado.
  - **Dirección IP estática de la Interfaz Ethernet:** Tipo string, longitud máxima 15 caracteres. Deberá representar una dirección IPv4 Válida. Por defecto tendrá el valor “192.168.0.100”.
  - **Máscara de subred estática de la Interfaz Ethernet:** Tipo string, longitud máxima 15 caracteres. Deberá representar una máscara de subred IPv4 Válida. Por defecto tendrá el valor “255.255.255.0”.
  - **Puerta de enlace estática de la Interfaz Ethernet:** Tipo string, longitud máxima 15 caracteres. Deberá representar una dirección IPv4 Válida. Por defecto tendrá el valor “192.168.0.1”.
  - **DNS Primario estático de la Interfaz Ethernet:** Tipo string, longitud máxima 15 caracteres. Deberá representar una dirección IPv4 Válida. Por defecto tendrá el valor “8.8.8.8”.
  - **DNS Secundario estático de la Interfaz Ethernet:** Tipo string, longitud máxima 15 caracteres. Deberá representar una dirección IPv4 Válida. Por defecto tendrá el valor “4.4.4.4”.
-

- **SSID de la Red Wi-Fi:** Tipo string alfanumérico, longitud máxima 25 caracteres. El valor por defecto es un string vacío.
- **Contraseña de la Red Wi-Fi:** Contraseña que utilizará el datalogger para conectarse a la red Wi-Fi. Tipo string alfanumérico, longitud máxima 25 caracteres. El valor por defecto es un string vacío.
- **Tipo de seguridad de la red Wi-Fi:** Tipo string. Indicará el esquema de seguridad a utilizar para conectarse a la red Wi-Fi. Únicamente podrá tomar los valores: “NINGUNA”, “WEP”, “WPA” y “WPA2”. Por defecto tendrá el valor “NINGUNA”.
- **Ciente DHCP Interfaz Wi-Fi Habilitado:** Campo booleano que indicará si la interfaz Wi-Fi del datalogger obtendrá una dirección IP y configuración de red en forma dinámica (verdadero) o utilizará la dirección IP estática configurada (falso). Por defecto estará deshabilitado.
- **Dirección IP estática de la Interfaz Wi-Fi:** Tipo string, longitud máxima 15 caracteres. Deberá representar una dirección IPv4 Válida. Por defecto tendrá el valor “192.168.0.101”.
- **Máscara de subred estática de la Interfaz Wi-Fi:** Tipo string, longitud máxima 15 caracteres. Deberá representar una máscara de subred IPv4 Válida. Por defecto tendrá el valor “255.255.255.0”.
- **Puerta de enlace estática de la Interfaz Wi-Fi:** Tipo string, longitud máxima 15 caracteres. Deberá representar una dirección IPv4 Válida. Por defecto tendrá el valor “192.168.0.1”.
- **DNS Primario estático de la Interfaz Wi-Fi:** Tipo string, longitud máxima 15 caracteres. Deberá representar una dirección IPv4 Válida. Por defecto tendrá el valor “8.8.8.8”.
- **DNS Secundario estático de la Interfaz Wi-Fi:** Tipo string, longitud máxima 15 caracteres. Deberá representar una dirección IPv4 Válida. Por defecto tendrá el valor “4.4.4.4”.
- **URL del servidor central:** Tipo string. Indicará la URL o el IP del servidor central al que deberán reportarse los dataloggers.
- **Puerto del servidor central:** Tipo numérico entero mayor a 0. Indicará el puerto TCP al que deberán conectarse los dataloggers para reportarse al servidor central. Por defecto tendrá el valor “80”.
- **Timeout de conexión al servidor:** Tipo numérico entero mayor a 0. Indica el tiempo en segundos durante el cual se intentará establecer la conexión con el servidor central. Por defecto tendrá el valor “60”.
- **Timeout de intercambio de datos con el servidor:** Tipo numérico entero mayor a 0. Indica el tiempo en segundos durante el cual la conexión con el servidor central deberá permanecer inactiva para que el datalogger detecte un problema de conexión. Por defecto tendrá el valor “120”.
- **Cantidad de reintentos de reconexión por ciclo:** Tipo numérico entero mayor a 0. Indica la cantidad de veces por ciclo de conexión que el datalogger intentará reconectarse con el servidor central. Pasado este número de intentos, el datalogger comenzará la espera para iniciar un nuevo ciclo de conexión. Por defecto tendrá el valor “5”.
- **Tiempo de espera entre reconexiones:** Tipo numérico entero mayor a 0. Indica el tiempo de espera en segundos entre intentos de reconexión dentro de un mismo ciclo. Por defecto tendrá el valor “120”.
- **Tiempo de espera para recomienzo de ciclo de conexión:** Tipo numérico entero mayor a 0. Indica el tiempo de espera en segundos entre ciclos de reconexión. Por defecto tendrá el valor “7200” (120 minutos).
- **Comentarios:** Tipo string, longitud máxima 255 caracteres.

#### 8.4.4.1 Relaciones con otras Entidades

Cada entidad “Configuración de red” deberá estar asignada a una única entidad “Datalogger” y viceversa. Es decir, cada datalogger deberá contar con una única configuración de red activa.

---

#### 8.4.5 Entidad: Configuración de Mediciones

Estas entidades representarán la configuración de las mediciones a obtener por los dataloggers. El servidor deberá proveer una página de ABM para esta entidad, la cual validará que los datos ingresados sean correctos. Deberá también permitir la duplicación de una entidad para generar una nueva sin que sea necesario ingresar todos los datos nuevamente.

Como mínimo deberá contener las siguientes propiedades:

- **Id de la entidad:** Primary Key. Número utilizado para identificar unívocamente la entidad. Autogenerado por el sistema y no modificable.
- **Periodo de Medición:** Tipo string. Indicará el periodo entre mediciones del datalogger en minutos. Únicamente podrá tomar los valores: "MINUTOS\_1", "MINUTOS\_5", "MINUTOS\_15", "MINUTOS\_30" y "MINUTOS\_60". Por defecto tendrá el valor "MINUTOS\_1"
- **Tensión del Banco de Baterías:** Tipo string. Indicará la tensión nominal del banco de baterías. Únicamente podrá tomar los valores: "BANCO12V", "BANCO24V" y "BANCO48V". Por defecto tendrá el valor "BANCO48V".
- **Tensión máxima del banco de baterías para el estado de carga "Muy Bajo":** Tipo numérico decimal mayor a 0. Indicará la tensión máxima para la cual se considerará que el banco de baterías se encuentra en el estado de carga "Muy Bajo" en Volts. Por defecto tendrá el valor "46".
- **Tensión máxima del banco de baterías para el estado de carga "Bajo":** Tipo numérico decimal mayor a 0. Indicará la tensión máxima para la cual se considerará que el banco de baterías se encuentra en el estado de carga "Bajo" en Volts. Por defecto tendrá el valor "47.6".
- **Tensión máxima del banco de baterías para el estado de carga "Medio":** Tipo numérico decimal mayor a 0. Indicará la tensión máxima para la cual se considerará que el banco de baterías se encuentra en el estado de carga "Medio" en Volts. Por defecto tendrá el valor "48.6".
- **Tensión máxima del banco de baterías para el estado de carga "Alto":** Tipo numérico decimal mayor a 0. Indicará la tensión máxima para la cual se considerará que el banco de baterías se encuentra en el estado de carga "Alto" en Volts. Por defecto tendrá el valor "49.2".
- **Coefficiente de corrección por temperatura de tensión de banco de baterías:** Tipo numérico decimal. Indicará el coeficiente de corrección por temperatura a utilizar para el cálculo de la tensión del banco de baterías (en mV/D°C, respecto a 25 °C). Por defecto tendrá el valor "-0.003".
- **Comentarios:** Tipo string, longitud máxima 255 caracteres.

##### 8.4.5.1 Relaciones con otras Entidades

Cada entidad "Configuración de Mediciones" deberá estar asignada a una única entidad "Datalogger" y viceversa. Es decir, cada datalogger deberá contar con una única configuración de mediciones activa.

#### 8.4.6 Entidad: Configuración de Alarmas

Estas entidades representarán la configuración de las alarmas a detectar por los dataloggers. El servidor deberá proveer una página de ABM para esta entidad, la cual validará que los datos ingresados sean correctos. Deberá también permitir la duplicación de una entidad para generar una nueva sin que sea necesario ingresar todos los datos nuevamente.

Como mínimo deberá contener las siguientes propiedades:

- **Id de la entidad:** Primary Key. Número utilizado para identificar unívocamente la entidad. Autogenerado por el sistema y no modificable.
  - **Tensión de alarma de baja batería:** Tipo numérico decimal mayor a 0. Indicará la tensión en Volts del banco de baterías para disparar la alarma de baja reserva de energía. Por defecto tendrá el valor "44.0".
-

- **Tiempo de alarma de baja batería:** Tipo numérico entero mayor a 0. Indicará el tiempo en segundos durante el cual la condición de baja batería deberá mantenerse para disparar la alarma. Por defecto tendrá el valor "15".
  - **Tensión de restablecimiento de alarma de baja batería:** Tipo numérico decimal mayor a 0. Indicará la tensión en Volts del banco de baterías para desactivar la condición de alarma de baja reserva de energía. Por defecto tendrá el valor "46.0".
  - **Tiempo de restablecimiento de alarma de baja batería:** Tipo numérico entero mayor a 0. Indicará el tiempo en segundos durante el cual la tensión mínima de restablecimiento de la alarma de baja batería deberá mantenerse para desactivar a la misma. Por defecto tendrá el valor "60".
  - **Alarma de baja batería habilitada:** Tipo booleano. Indicará si la alarma de baja batería está habilitada (true) o deshabilitada (false). Por defecto estará habilitada.
  - **Tensión de alarma de sobretensión en baterías:** Tipo numérico decimal mayor a 0. Indicará la tensión mínima en Volts del banco de baterías para disparar la alarma de sobretensión. Por defecto tendrá el valor "58.0".
  - **Tiempo de alarma de sobretensión en baterías:** Tipo numérico entero mayor a 0. Indicará el tiempo en segundos durante el cual la condición de sobretensión en baterías deberá mantenerse para disparar la alarma. Por defecto tendrá el valor "15".
  - **Tensión de restablecimiento de alarma de sobretensión en baterías:** Tipo numérico decimal mayor a 0. Indicará la tensión máxima en Volts del banco de baterías para desactivar la condición de alarma de sobretensión en baterías. Por defecto tendrá el valor "52.0".
  - **Tiempo de restablecimiento alarma de sobretensión en baterías:** Tipo numérico entero mayor a 0. Indicará el tiempo en segundos durante el cual la tensión del banco de baterías deberá permanecer por debajo de la tensión de restablecimiento de la alarma para desactivar la misma. Por defecto tendrá el valor "60".
  - **Alarma de sobretensión en baterías habilitada:** Tipo booleano. Indicará si la alarma de sobretensión en baterías está habilitada (true) o deshabilitada (false). Por defecto estará habilitada.
  - **Corriente de alarma de sobrecorriente del regulador solar:** Tipo numérico decimal mayor a 0. Indicará la corriente en Amperes para la detección de sobrecorriente de carga del regulador solar. Por defecto tendrá el valor "280.0".
  - **Tiempo de alarma de sobrecorriente de carga del regulador solar:** Tipo numérico entero mayor a 0. Indicará el tiempo en segundos durante el cual la condición de sobrecorriente de carga del regulador solar deberá mantenerse para disparar la alarma. Por defecto tendrá el valor "15".
  - **Corriente de restablecimiento de alarma de sobrecorriente del regulador solar:** Tipo numérico decimal mayor a 0. Indicará la corriente en Amperes debajo de la cual se deberá mantener la corriente de carga del regulador solar para desactivar la alarma de sobrecorriente. Por defecto tendrá el valor "150.0".
  - **Tiempo de restablecimiento de alarma de sobrecorriente del regulador solar:** Tipo numérico entero mayor a 0. Indicará el tiempo en segundos durante el cual la corriente de restablecimiento de la alarma de sobrecorriente de carga del regulador solar no deberá superarse para desactivar la alarma. Por defecto tendrá el valor "60".
  - **Alarma de sobrecorriente del regulador solar habilitada:** Tipo booleano. Indicará si la alarma de sobrecorriente de carga del regulador solar está habilitada (true) o deshabilitada (false). Por defecto estará habilitada.
  - **Corriente de alarma de sobrecorriente del cargador de baterías:** Tipo numérico decimal mayor a 0. Indicará la corriente en Amperes para la detección de sobrecorriente de carga del cargador de baterías. Por defecto tendrá el valor "280.0".
-

- **Tiempo de alarma de sobrecorriente del cargador de baterías:** Tipo numérico entero mayor a 0. Indicará el tiempo en segundos durante el cual la condición de sobrecorriente del cargador de baterías deberá mantenerse para disparar la alarma. Por defecto tendrá el valor "15".
  - **Corriente de restablecimiento de alarma de sobrecorriente del cargador de baterías:** Tipo numérico decimal mayor a 0. Indicará la corriente en Amperes debajo de la cual se deberá mantener la corriente del cargador de baterías para desactivar la alarma de sobrecorriente. Por defecto tendrá el valor "150.0".
  - **Tiempo de restablecimiento de alarma de sobrecorriente del cargador de baterías:** Tipo numérico entero mayor a 0. Indicará el tiempo en segundos durante el cual la corriente de restablecimiento de la alarma de sobrecorriente del cargador de baterías no deberá superarse para desactivar la alarma. Por defecto tendrá el valor "60".
  - **Alarma de sobrecorriente del cargador de baterías habilitada:** Tipo booleano. Indicará si la alarma de sobrecorriente del cargador de baterías está habilitada (true) o deshabilitada (false). Por defecto estará habilitada.
  - **Corriente de alarma de sobrecorriente de descarga de baterías:** Tipo numérico decimal mayor a 0. Indicará el valor absoluto de la corriente en Amperes para la detección de sobrecorriente de descarga del banco de baterías. Por defecto tendrá el valor "280.0".
  - **Tiempo de alarma de sobrecorriente de descarga de baterías:** Tipo numérico entero mayor a 0. Indicará el tiempo en segundos durante el cual la condición de sobrecorriente de descarga de baterías deberá mantenerse para disparar la alarma. Por defecto tendrá el valor "15".
  - **Corriente de restablecimiento de alarma de sobrecorriente de descarga de baterías:** Tipo numérico decimal mayor a 0. Indicará la corriente en Amperes debajo de la cual se deberá mantener la corriente de descarga de baterías (en valor absoluto) para desactivar la alarma de sobrecorriente. Por defecto tendrá el valor "150.0".
  - **Tiempo de restablecimiento de alarma de sobrecorriente de descarga de baterías:** Tipo numérico entero mayor a 0. Indicará el tiempo en segundos durante el cual la corriente de restablecimiento de la alarma de sobrecorriente de descarga de baterías no deberá superarse para desactivar la alarma. Por defecto tendrá el valor "60".
  - **Alarma de sobrecorriente de descarga de baterías habilitada:** Tipo booleano. Indicará si la alarma de sobrecorriente de descarga de baterías está habilitada (true) o deshabilitada (false). Por defecto estará habilitada.
  - **Potencia mínima de alarma de potencia del regulador solar diurna nula:** Tipo numérico decimal mayor a 0. Indicará la potencia mínima en Watts que el regulador solar deberá entregar durante el horario diurno para no disparar la alarma de potencia solar diurna nula. Por defecto tendrá el valor "50.0".
  - **Tiempo de alarma de potencia del regulador solar diurna nula:** Tipo numérico entero mayor a 0. Indicará el tiempo en segundos durante el cual la condición de potencia de carga del regulador solar diurna nula deberá mantenerse para disparar la alarma. Por defecto tendrá el valor "3600".
  - **Potencia de restablecimiento de alarma de potencia del regulador solar diurna nula:** Tipo numérico decimal mayor a 0. Indicará la potencia de carga del regulador solar (en Watts) que deberá ser superada para desactivar la alarma de potencia diurna nula de carga del regulador solar. Por defecto tendrá el valor "250.0".
  - **Tiempo de restablecimiento de alarma de potencia del regulador solar diurna nula:** Tipo numérico entero mayor a 0. Indicará el tiempo en segundos durante el cual la potencia de carga del regulador solar deberá mantenerse por encima del valor de restablecimiento de la alarma para desactivar la misma. Por defecto tendrá el valor "600".
-

- **Comienzo del horario diurno:** Tipo string ó "TIMESTAMP" según formato "HH:mm:ss". Indicará la hora de comienzo del horario diurno para la detección de potencia diurna nula en el regulador solar. Por defecto tendrá el valor "10:00:00".
  - **Finalización del horario diurno:** Tipo string ó "TIMESTAMP" según formato "HH:mm:ss". Indicará la hora de finalización para la detección de potencia diurna nula en el regulador solar. Por defecto tendrá el valor "16:00:00".
  - **Alarma de potencia del regulador solar diurna nula habilitada:** Tipo booleano. Indicará si la alarma de potencia de regulador solar diurna nula está habilitada (true) o deshabilitada (false). Por defecto estará habilitada.
  - **Potencia mínima de alarma de potencia nula a la salida del inversor:** Tipo numérico decimal mayor a 0. Indicará la potencia mínima en Watts que el inversor debe entregar a su salida para detectar su correcto funcionamiento. Por defecto tendrá el valor "5.0".
  - **Tiempo de alarma de potencia nula a la salida del inversor:** Tipo numérico entero mayor a 0. Indicará el tiempo en segundos durante el cual la condición de potencia nula a la salida del inversor deberá mantenerse para disparar la alarma. Por defecto tendrá el valor "3600".
  - **Potencia de restablecimiento de alarma de potencia nula a la salida del inversor:** Tipo numérico decimal mayor a 0. Indicará la potencia de salida del inversor (en Watts) que deberá ser superada para desactivar la alarma de potencia nula a la salida del inversor. Por defecto tendrá el valor "20.0".
  - **Tiempo de restablecimiento de alarma de potencia nula a la salida del inversor:** Tipo numérico entero mayor a 0. Indicará el tiempo en segundos durante el cual la potencia de salida del inversor deberá mantenerse por encima del valor de restablecimiento de la alarma para desactivar la misma. Por defecto tendrá el valor "60".
  - **Alarma de potencia nula a la salida de inversor habilitada:** Tipo booleano. Indicará si la alarma de potencia nula a la salida del inversor está habilitada (true) o deshabilitada (false). Por defecto estará habilitada.
  - **Corriente de alarma de sobrecorriente a la salida del inversor:** Tipo numérico decimal mayor a 0. Indicará la corriente en Amperes para la detección de sobrecorriente a la salida del inversor. Por defecto tendrá el valor "45.0".
  - **Tiempo de alarma de sobrecorriente a la salida del inversor:** Tipo numérico entero mayor a 0. Indicará el tiempo en segundos durante el cual la condición de sobrecorriente a la salida del inversor deberá mantenerse para disparar la alarma. Por defecto tendrá el valor "5".
  - **Corriente de restablecimiento de alarma de sobrecorriente a la salida del inversor:** Tipo numérico decimal mayor a 0. Indicará la corriente en Amperes debajo de la cual se deberá mantener la corriente a la salida del inversor para desactivar la alarma de sobrecorriente. Por defecto tendrá el valor "40.0".
  - **Tiempo de restablecimiento de alarma de sobrecorriente a la salida del inversor:** Tipo numérico entero mayor a 0. Indicará el tiempo en segundos durante el cual la corriente de restablecimiento de la alarma de sobrecorriente a la salida del inversor no deberá superarse para desactivar la alarma. Por defecto tendrá el valor "60".
  - **Alarma de sobrecorriente a la salida del inversor habilitada:** Tipo booleano. Indicará si la alarma de sobrecorriente a la salida del inversor está habilitada (true) o deshabilitada (false). Por defecto estará habilitada.
  - **Temperatura máxima de alarma de sobretemperatura del banco de baterías:** Tipo numérico decimal mayor a 0. Indicará la temperatura máxima en °C por encima de la cual se deberá mantener la temperatura del banco de baterías para disparar la alarma. Por defecto tendrá el valor "40.0".
  - **Tiempo de alarma de sobretemperatura del banco de baterías:** Tipo numérico entero mayor a 0. Indicará el tiempo en segundos durante el cual la condición de sobretemperatura
-

en el banco de baterías deberá mantenerse para disparar la alarma. Por defecto tendrá el valor “300”.

- **Temperatura de restablecimiento de alarma de sobretemperatura del banco de baterías:** Tipo numérico decimal mayor a 0. Indicará la temperatura máxima en °C por debajo de la cual se deberá mantener la temperatura del banco de baterías para desactivar la alarma. Por defecto tendrá el valor “30.0”.
- **Tiempo de restablecimiento de alarma de sobretemperatura del banco de baterías:** Tipo numérico entero mayor a 0. Indicará el tiempo en segundos durante el cual la temperatura del banco de baterías deberá mantenerse por debajo del valor de restablecimiento para desactivar la alarma. Por defecto tendrá el valor “300”.
- **Alarma de sobretemperatura del banco de baterías habilitada:** Tipo booleano. Indicará si la alarma de sobretemperatura del banco de baterías está habilitada (true) o deshabilitada (false). Por defecto estará habilitada.
- **Temperatura mínima de alarma de baja temperatura del banco de baterías:** Tipo numérico decimal mayor a 0. Indicará la temperatura mínima en °C por debajo de la cual se deberá mantener la temperatura del banco de baterías para disparar la alarma. Por defecto tendrá el valor “5.0”.
- **Tiempo de alarma de baja temperatura del banco de baterías:** Tipo numérico entero mayor a 0. Indicará el tiempo en segundos durante el cual la condición de baja temperatura en el banco de baterías deberá mantenerse para disparar la alarma. Por defecto tendrá el valor “300”.
- **Temperatura de restablecimiento de alarma de baja temperatura del banco de baterías:** Tipo numérico decimal mayor a 0. Indicará la temperatura máxima en °C por encima de la cual se deberá mantener la temperatura del banco de baterías para desactivar la alarma. Por defecto tendrá el valor “10.0”.
- **Tiempo de restablecimiento de alarma de baja temperatura del banco de baterías:** Tipo numérico entero mayor a 0. Indicará el tiempo en segundos durante el cual la temperatura del banco de baterías deberá mantenerse por encima del valor de restablecimiento para desactivar la alarma. Por defecto tendrá el valor “300”.
- **Alarma de baja temperatura del banco de baterías habilitada:** Tipo booleano. Indicará si la alarma de baja temperatura del banco de baterías está habilitada (true) o deshabilitada (false). Por defecto estará habilitada.
- **Comentarios:** Tipo string, longitud máxima 255 caracteres.

#### 8.4.6.1 Relaciones con otras Entidades

Cada entidad “Configuración de Alarmas” deberá estar asignada a una única entidad “Datalogger” y viceversa. Es decir, cada datalogger deberá contar con una única configuración de alarmas activa.

#### 8.4.7 Entidad: Configuración de Eventos

Estas entidades representarán la configuración de los eventos a detectar por los dataloggers. El servidor deberá proveer una página de ABM para esta entidad, la cual validará que los datos ingresados sean correctos. Deberá también permitir la duplicación de una entidad para generar una nueva sin que sea necesario ingresar todos los datos nuevamente.

Como mínimo deberá contener las siguientes propiedades:

- **Id de la entidad:** Primary Key. Número utilizado para identificar unívocamente la entidad. Autogenerado por el sistema y no modificable.
  - **Reporte de encendido habilitado:** Tipo booleano. Indicará si el reporte del evento de encendido está habilitado (true) o deshabilitado (false). Por defecto estará habilitado.
  - **Reporte de reseteo de watchdog interno habilitado:** Tipo booleano. Indicará si el reporte del evento de reseteo por watchdog interno está habilitado (true) o deshabilitado (false). Por defecto estará habilitado.
-

- **Reporte de reseteo de watchdog externo habilitado:** Tipo booleano. Indicará si el reporte del evento de reseteo por watchdog externo está habilitado (true) o deshabilitado (false). Por defecto estará habilitado.
- **Reporte de reseteo de configuración a valores por defecto habilitado:** Tipo booleano. Indicará si el reporte del evento de reseteo de configuración a los valores por defecto está habilitado (true) o deshabilitado (false). Por defecto estará habilitado.
- **Reporte de conexión a red habilitado:** Tipo booleano. Indicará si el reporte del evento de conexión a la red está habilitado (true) o deshabilitado (false). Por defecto estará habilitado.
- **Reporte de desconexión de la red habilitado:** Tipo booleano. Indicará si el reporte del evento de desconexión de la red está habilitado (true) o deshabilitado (false). Por defecto estará habilitado.
- **Espacio libre mínimo en la memoria interna:** Tipo numérico entero mayor a 0. Indicará el espacio libre de memoria interna mínimo (en kB) para reportar dicha situación al servidor. Por defecto tendrá el valor "100".
- **Reporte de bajo espacio libre en la memoria interna habilitado:** Tipo booleano. Indicará si el reporte del evento de baja memoria interna está habilitado (true) o deshabilitado (false). Por defecto estará habilitado.
- **Reporte de pérdida de datos habilitado:** Tipo booleano. Indicará si el reporte del evento pérdida de datos debido a bajo o nulo espacio libre en la memoria interna está habilitado (true) o deshabilitado (false). Por defecto estará habilitado.
- **Comentarios:** Tipo string, longitud máxima 255 caracteres.

#### 8.4.7.1 Relaciones con otras Entidades

Cada entidad "Configuración de Eventos" deberá estar asignada a una única entidad "Datalogger" y viceversa. Es decir, cada datalogger deberá contar con una única configuración de eventos activa.

#### 8.4.8 Entidad: Medición

Estas entidades representarán las mediciones obtenidas por los dataloggers y reportadas al servidor. Si bien estas entidades serán generadas automáticamente por el servidor al recibir los reportes de medición de los dataloggers, el servidor deberá proveer una página de ABM para esta entidad, la cual validará que los datos ingresados sean correctos.

Como mínimo deberá contener las siguientes propiedades:

- **Id de la entidad:** Primary Key. Número utilizado para identificar unívocamente la entidad. Autogenerado por el sistema y no modificable.
  - **Fecha y hora de medición:** Campo del tipo "DATETIME" ó "TIMESTAMP" según formato "YYYY-MM-DDTHH:mm:ss". Indicará la hora y fecha de la medición realizada.
  - **Tensión de los paneles fotovoltaicos:** Tipo numérico decimal. Tensión en Volts.
  - **Corriente entregada por los paneles fotovoltaicos:** Tipo numérico decimal. Corriente en Amperes.
  - **Potencia Instantánea entregada por el regulador solar:** Tipo numérico decimal. Potencia en Watts.
  - **Energía diaria generada por los paneles fotovoltaicos:** Tipo numérico decimal. Energía en Watts-Hora.
  - **Tensión del banco de baterías:** Tipo numérico decimal. Tensión en Volts.
  - **Corriente de carga y descarga del banco de baterías:** Tipo numérico decimal. Corriente en Amperes. Valores positivos indican carga del banco de baterías, valores negativos descarga.
  - **Estado de carga del banco de baterías:** Tipo numérico entero. Indicará el estado de carga según la convención: "0=muy bajo, 1=bajo, 2=medio, 3=alto, 4=muy alto".
  - **Corriente entregada por el cargador de baterías:** Tipo numérico decimal. Corriente en Amperes.
  - **Temperatura del banco de baterías:** Tipo numérico decimal. Temperatura en °C.
-



- **Tensión alterna de consumos de usuario:** Tipo numérico decimal. Tensión alterna eficaz en Volts.
- **Corriente alterna de consumos de usuario:** Tipo numérico decimal. Corriente alterna eficaz en Amperes.
- **Potencia instantánea de consumos de usuario:** Tipo numérico decimal. Potencia en Watts.
- **Energía diaria consumida:** Tipo numérico decimal. Energía en Watts-Hora.
- **Posición de la llave selectora:** Tipo numérico entero. Indicará la posición de la llave selectora: “0=sin conexión,1=Inversor, 2=Generador”

#### 8.4.8.1 Relaciones con otras Entidades

Cada entidad “Medición” deberá estar asignada a una única entidad “Datalogger”. Sin embargo, cada datalogger podrá tener asignadas múltiples entidades “Medición”.

#### 8.4.9 Entidad: Alarma

Estas entidades representarán las alarmas detectadas por los dataloggers y reportadas al servidor. Si bien estas entidades serán generadas automáticamente por el servidor al recibir los reportes de alarmas de los dataloggers, el servidor deberá proveer una página de ABM para esta entidad, la cual validará que los datos ingresados sean correctos.

Como mínimo deberá contener las siguientes propiedades:

- **Id de la entidad:** Primary Key. Número utilizado para identificar unívocamente la entidad. Autogenerado por el sistema y no modificable.
- **Fecha y hora de alarma:** Campo del tipo “DATETIME” ó “TIMESTAMP” según formato “YYYY-MM-DDTHH:mm:ss”. Indicará la hora y fecha de comienzo de la condición de alarma.
- **Código de alarma:** Tipo numérico entero. Codificará la condición de alarma según la siguiente tabla:

Alarma	Código	Valor a Reportar
Baja tensión en banco de baterías	100	Tensión del banco de baterías
Sobretensión en banco de baterías	101	Tensión del banco de baterías
Sobrecorriente de carga del regulador solar	102	Corriente del regulador solar
Sobrecorriente de carga del cargador de baterías	103	Corriente del cargador de baterías
Sobrecorriente de descarga del banco de baterías	104	Corriente del banco de baterías
Temperatura alta en el banco de baterías	105	Temperatura del banco de baterías
Temperatura baja en el banco de baterías	105	Temperatura del banco de baterías
Potencia nula diurna a la salida del regulador solar	200	Potencia a la salida del regulador solar
Potencia nula a la salida del inversor	300	Potencia a la salida del inversor
Sobrecorriente a la salida del inversor	301	Corriente a la salida del inversor

- **Valor registrado:** Tipo numérico decimal. Será el valor que disparó (o desactivó) la condición de alarma, y su interpretación dependerá del tipo de alarma, según la tabla anterior.
- **Alarma disparada:** Tipo booleano. Indicará si la alarma se disparó (true) o si por el contrario la misma ha sido restablecida (false).

#### 8.4.9.1 Relaciones con otras Entidades

Cada entidad “Alarma” deberá estar asignada a una única entidad “Datalogger”. Sin embargo, cada datalogger podrá tener asignadas múltiples entidades “Alarma”.

#### 8.4.10 Entidad: Evento

Estas entidades representarán los eventos detectados por los dataloggers y reportadas al servidor. Si bien estas entidades serán generadas automáticamente por el servidor al recibir los reportes de

eventos de los dataloggers, el servidor deberá proveer una página de ABM para esta entidad, la cual validará que los datos ingresados sean correctos.

Como mínimo deberá contener las siguientes propiedades:

- **Id de la entidad:** Primary Key. Número utilizado para identificar unívocamente la entidad. Autogenerado por el sistema y no modificable.
- **Fecha y hora del evento:** Campo del tipo “DATETIME” ó “TIMESTAMP” según formato “YYYY-MM-DDTHH:mm:ss”. Indicará la hora y fecha de comienzo de detección del evento.
- **Código de evento:** Tipo numérico entero. Codificara el evento detectado según la siguiente tabla:

Evento	Código
Encendido del sistema	100
Apagado del sistema	101
Reseteo del sistema por watchdog interno	102
Reseteo del sistema por watchdog externo	103
Reseteo del sistema a valores por defecto	104
Conexión a la red establecida	200
Pérdida de conexión con la red	201
Alarma de baja memoria disponible	300
Alarma de pérdida de datos por sobre-escritura	301

#### 8.4.10.1 Relaciones con otras Entidades

Cada entidad “Evento” deberá estar asignada a una única entidad “Datalogger”. Sin embargo, cada datalogger podrá tener asignadas múltiples entidades “Evento”.

#### 8.4.11 Entidad: Firmware

Estas entidades representarán a las distintas versiones de firmware del datalogger, las cuales se utilizarán para realizar las actualizaciones de los mismos. El servidor deberá proveer una página de ABM para esta entidad, permitiendo subir un archivo de firmware por cada entidad.

Como mínimo deberá contener las siguientes propiedades:

- **Id de la entidad:** Primary Key. Número utilizado para identificar unívocamente la entidad. Autogenerado por el sistema y no modificable.
- **Fecha de firmware:** Campo del tipo “DATETIME” ó “TIMESTAMP” según formato “YYYY-MM-DDTHH:mm:ss”. Indicará la hora y fecha de subida del firmware al sistema (autogenerado).
- **Versión de firmware:** Tipo string, longitud máxima 20 caracteres.
- **Ruta al archivo de firmware:** Tipo string, longitud máxima 255 caracteres. Indicará la ruta (path) al archivo de firmware. Autogenerado por el sistema.
- **Comentarios:** Tipo string, longitud máxima 255 caracteres.

#### 8.4.11.1 Relaciones con otras Entidades

Cada entidad “Firmware” podrá estar asignada a múltiples entidades “Datalogger”. Sin embargo, cada datalogger podrá tener sólo asignada una única entidad “Firmware”.

### 8.5 Tipos de usuario del sistema

El sistema deberá contar con tres tipos de niveles de usuario, cada uno con distintos permisos, según la siguiente tabla:

Tipo de usuario	Permisos
Administrador del sistema	Control Total.
Usuario para configuración y consultas	Lectura y escritura de mediciones, alarmas, eventos y configuraciones.
Usuario para consultas	Lectura de mediciones, alarmas, eventos y configuraciones.

Las contraseñas de los usuarios deberán guardarse en la base de datos utilizando algún tipo de encriptación, del estilo “Hash MD5” o similar.

#### 8.6 Parámetros de configuración del sistema

El servidor web deberá permitir la configuración de sus múltiples parámetros de configuración interna que afecten su funcionamiento a través de una página web.

Asimismo, la configuración de los parámetros de comunicación con los dataloggers deberá ser configurable (por ejemplo, timeouts de inactividad durante el envío de datos, etc.).

#### 8.7 Actualización del software del servidor

El software del servidor web deberá poder ser actualizable en forma remota subiendo un archivo (por ejemplo, del estilo “WAR” utilizado en servidores Apache Tomcat) a través de una interfaz de administración web. El proceso de “deployment” deberá luego estar automatizado y no deberá incurrir en pérdida o borrado de los registros preexistentes en la base de datos.

#### 8.8 Gráficos y reportes

El servidor deberá proveer la funcionalidad de realizar consultas y gráficos de las variables registradas por los dataloggers.

Para ello, deberá tener una interfaz amigable (al estilo “dashboard”), donde se puedan seleccionar el ID del datalogger a consultar, el rango de fechas y las variables a graficar (mediciones, alarmas, eventos, etc.).

Asimismo, deberá permitir filtrar mediciones por los siguientes criterios:

- Tipo y valores de variables máximos y mínimos (múltiples variables y condiciones).
- Tipo de alarma.
- Tipo de evento.

Deberá también permitirse la descarga de los datos graficados en formato “csv” (valores separados por coma) para su posterior análisis y tratamiento.

#### 8.9 Administración de firmware de los dataloggers

El sistema deberá permitir administrar múltiples versiones de firmware, de forma tal de proveer la funcionalidad de actualización de los dataloggers instalados. Para ello deberá permitir subir un archivo al ingresar una nueva entidad “Firmware” (sección 8.4.11) al sistema.

La orden de actualización de firmware a los dataloggers no será generada en forma automática por el sistema, sino que la misma deberá ingresarse manualmente, posibilitando la actualización de múltiples dataloggers a través con una única orden (batch).

#### 8.10 Loggeo de comunicación

De forma tal de facilitar el proceso de debuggeo de la comunicación con los dataloggers, el servidor deberá proveer una pantalla de loggeo de mensajes, advertencias y errores. Deberá poder seleccionarse el nivel de loggeo de cada datalogger en particular, de forma tal de evitar confusiones de interpretación.

Deberán también loggearse timeouts de comunicación, valores recibidos inválidos y otro tipo de información que sea pertinente.

**Importante:** la pantalla de loggeo deberá ser accesible vía web, actualizándose en forma automática. Asimismo, los archivos de log deberán quedar guardados en el servidor para consultas posteriores.

#### 8.11 Compatibilidad con browsers y dispositivos móviles

De forma tal de poder acceder al servidor central de prueba desde cualquier PC o dispositivo móvil, el mismo deberá utilizar tecnologías web no propietarias y Open Source. Debido a esto, las páginas web servidas por el servidor central deberán ser compatibles con HTML 4 y JavaScript 1.8.5. La interfaz gráfica deberá estar basada en jQuery y CSS 3.0.

**Importante:** La interfaz gráfica deberá estar basada en tecnologías AJAX o similar, es decir, deberá actualizar la información mostrada en pantalla automáticamente sin necesidad de que el usuario recargue la página desde el navegador.

---

## **9 Frameworks y hosteo en la “nube”**

El servidor deberá basar su funcionamiento en tecnologías de software que no requieran el pago de una licencia. Por ejemplo, no deberán utilizarse lenguajes, servidores web, o motores de bases de datos propietarias (del estilo Oracle o similar).

Las tecnologías seleccionadas bajo este criterio deberán permitir que el servidor sea hosteado en servidores en la nube (del tipo VPS, AWS de Amazon o Azure de Microsoft).

## 10 Entregables

### 10.1 Imagen máquina virtual

Para facilitar la instalación y ejecución del servidor central de prueba en cualquier tipo de PC, deberá entregarse una imagen de una máquina virtual con el servidor central de prueba funcionando. Dicha imagen deberá poseer todas las dependencias de software (sistema operativo, SDKs, etc.) y servidores instalados y listos para comenzar a funcionar. De esta forma el proveedor puede abstraerse del sistema (hardware) en el que finalmente correrá el servidor.

**Importante:** El formato de la imagen deberá ser compatible con “Oracle VM Virtual Box”.

### 10.2 Esquema entidad relación de la base de datos

Deberá entregarse el esquema entidad relación utilizado en la base de datos, de forma tal de permitir realizar consultas en forma directa sobre la misma utilizando herramientas externas.

### 10.3 Manual de usuario

Deberá entregarse un manual de usuario el cual indique en rasgos generales el funcionamiento del sistema haciendo hincapié en los aspectos menos intuitivos del mismo.

### 10.4 Procedimiento de instalación dentro de la máquina virtual

Deberá entregarse un documento con el procedimiento de instalación, configuración y puesta en marcha de los distintos servidores y dependencias de software que deben ser instalados **dentro** la máquina virtual para llegar a ejecutar el servidor tomando como punto de partida una máquina virtual vacía.

Este procedimiento deberá especificar el sistema operativo a utilizar, los SDKs y servidores a instalar, así como también la versión y configuración de cada componente.

## 10.5 Ensayos

El oferente deberá especificar todos los ensayos y pruebas de los equipos que ha de realizar para probar la calidad y el cumplimiento satisfactorio de las condiciones funcionales y operativas para cada parte de la provisión y para el conjunto del sistema.

El oferente deberá disponer como mínimo la realización de los ensayos que se detallan:

Del total del suministro de dataloggers se seleccionará una muestra equivalente al 1% y se conectarán al servidor de prueba a través de una conexión Wi-Fi. Los ensayos comprenderán:

- Verificación de los valores de medición dentro de los rangos especificados.
  - Consumo en stand by dentro del valor especificado.
  - Consumo en operación dentro del valor especificado.
  - Actualización de firmware.
  - Pruebas de conexión y comunicación (Wi-Fi y puerto ethernet).
  - Pruebas de funcionalidad de la página web de configuración.
  - **Monitoreo de recursos del servidor de prueba (Profiling):** Se deberán monitorear los recursos de memoria, CPU, disco rígido y red utilizados por el servidor, de forma tal de verificar que no existan “memory leaks” o conexiones inactivas que proliferen innecesariamente. Para ello se recomienda la utilización de herramientas de profiling que permitan analizar los recursos utilizados por el servidor ante gran cantidad de conexiones y pedidos de los dataloggers.
  - **Informe de recursos:** A partir de los análisis de profiling del servidor de prueba, se deberá entregar un informe donde se detallen los requerimientos de recursos del mismo, especificando las condiciones de prueba del mismo (por ejemplo, cantidad de pedidos de conexión por segundo, etc).
  - **Pruebas de comunicación con el servidor de prueba:** visualización de datos, tendencias y alarmas.
-

- **Pruebas de estabilidad:** Se deberá presentar un informe integral de funcionalidad de los dataloggers en conjunto con el servidor de prueba funcionando ininterrumpidamente por un período de 15 días. La estabilidad del servidor deberá probarse "bajo carga". Esto significa que deberá verificarse el correcto funcionamiento del mismo ante los pedidos simultáneos (requests) de "dataloggers virtuales" que imiten el comportamiento de los dataloggers reales con datos de prueba (sumados a los dataloggers reales pertenecientes a la muestra). A tal efecto, se recomienda desarrollar una aplicación con varios hilos (threads) que actúen como clientes del servidor siguiendo el protocolo de los dataloggers. Deberán poder atenderse hasta 100 conexiones simultáneas.

### 10.6 Garantía

El oferente deberá garantizar por defectos de fabricación por el término de dos (2) años a partir de la fecha de entrega.

Todas las garantías mencionadas deberán ser suministradas al comprador al momento de la firma del contrato.

En caso de productos que no sean fabricados en el país del contratante se exige la designación de un representante local para reclamos en garantía.

Se solicita un seguro de caución por el 10 % del monto del contrato.

---

**Anexo 1****FORMULARIO DE LA OFERTA**

*[El Licitante completará este formulario de acuerdo con las instrucciones indicadas. No se permitirán alteraciones a este formulario ni se aceptarán substituciones.]*

Fecha: *[Indicar la fecha (día, mes y año) de la presentación de la oferta]*  
LPN No. : *[indicar el número del proceso licitatorio]*  
Llamado a Licitación No.: *[indicar el No. del Llamado]*

A: *[nombre completo del Comprador]*

Nosotros, los suscritos, declaramos que:

- (a) Hemos examinado y no hallamos objeción alguna a los documentos de licitación, incluso sus Enmiendas Nos. \_\_\_\_\_ *[indicar el número y la fecha de emisión de cada Enmienda];*
  - (b) Ofrecemos proveer los siguientes Bienes y Servicios Conexos de conformidad con los Documentos de Licitación y de acuerdo con el Plan de Entregas establecido en la Lista de Bienes: \_\_\_\_\_ *[indicar una descripción breve de los bienes y servicios conexos];*
  - (c) El precio total de nuestra oferta, excluyendo cualquier descuento ofrecido en el rubro (d) a continuación es: \_\_\_\_\_ *[indicar el precio total de la oferta en palabras y en cifras, en pesos argentinos];*
  - (d) Nuestra oferta se mantendrá vigente por el período establecido en la Subcláusula 3.1.2 de la Sección B, a partir de la fecha límite fijada para la presentación de las ofertas de conformidad con la Subcláusula 3.1.1. Esta oferta nos obligará y podrá ser aceptada en cualquier momento antes de la expiración de dicho período;
  - (e) Si nuestra oferta es aceptada, nos comprometemos a obtener una Garantía de Cumplimiento del Contrato de conformidad con la Subcláusula 3.9.3 de la Sección B;
  - (f) Los suscritos, incluyendo todos los subcontratistas o proveedores requeridos para ejecutar cualquier parte del Contrato, tenemos nacionalidad de países elegibles \_\_\_\_\_ *[indicar la nacionalidad del Licitante, incluso la de todos los miembros que comprende el Licitante, si el Licitante es una Asociación en Participación o Consorcio, y la nacionalidad de cada subcontratista y proveedor]*
  - (g) No tenemos conflicto de intereses de conformidad con la Subcláusula 1.5.2 de la Sección A;
  - (h) Nuestra empresa, sus afiliados o subsidiarias, incluyendo todos los subcontratistas o proveedores para ejecutar cualquier parte del Contrato, no han sido declarados inelegibles por el Banco, bajo las leyes del país del Comprador o normativas oficiales, de conformidad con la Subcláusula 1.5.3 de la Sección A;
  - (i) Las siguientes comisiones, gratificaciones u honorarios han sido pagados o serán pagados en relación con el proceso de esta licitación o ejecución del Contrato: *[indicar el nombre completo de cada receptor, su dirección completa, la razón por la cual se pagó cada comisión o gratificación y la cantidad y moneda de cada dicha comisión o gratificación]*
-

Nombre del Receptor	Dirección	Concepto	Monto
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

(Si no han sido pagadas o no serán pagadas, indicar “ninguna”.)

- (j) Entendemos que esta oferta, junto con su debida aceptación por escrito incluida en la notificación de adjudicación, constituirán una obligación contractual entre nosotros, hasta que el Contrato formal haya sido perfeccionado por las partes.
- (k) Entendemos que ustedes no están obligados a aceptar la oferta evaluada más baja ni ninguna otra oferta que reciban.

Firma: \_\_\_\_\_ [indicar el nombre completo de la persona cuyo nombre y calidad se indican]

En calidad de \_\_\_\_\_ [indicar la capacidad jurídica de la persona que firma el Formulario de la Oferta]

Nombre: \_\_\_\_\_ [indicar el nombre completo de la persona que firma el Formulario de la Oferta]

Debidamente autorizado para firmar la oferta por y en nombre de: [indicar el nombre completo del Licitante]

El día \_\_\_\_\_ del mes \_\_\_\_\_ del año \_\_\_\_\_ [indicar la fecha de la firma]

---



**Anexo 2**  
**LISTA DE PRECIOS**

<i>Monedas de acuerdo con la Subcláusula 2.2.1 de la Sección B</i>							<i>Fecha: _____</i>
							<i>LPN No: _____</i>
							<i>Lote No.: _____</i>
							<i>Página N° ____ de ____</i>
1	2	3	4	5	6	7	8
<i>No. de Artículo</i>	<i>Descripción de los Bienes</i>	<i>Fecha de Entrega según Definición de Incoterms</i>	<i>Cantidad y Unidad Física</i>	<i>Precio Unitario DDP de Cada Artículo</i>	<i>Precio Total DDP por Cada Artículo (Col. 4x5)</i>	<i>Impuestos</i>	<i>Porcentaje (%) alícuota de IVA</i>
<i>Item 1</i>	<i>Equipos datalogger para escuelas rurales</i>	<i>[indicar la fecha de entrega ofertada]</i>	<i>500</i>	<i>[indicar precio unitario DDP]</i>	<i>[indicar precio total DDP por cada artículo]</i>	<i>[Indicar el monto correspondiente a los impuestos]</i>	<i>[Indicar el porcentaje correspondiente a la alícuota del IVA]</i>
<i>Item 2</i>	<i>Desarrollo de software en soporte físico</i>	<i>[indicar la fecha de entrega ofertada]</i>	<i>1</i>	<i>[indicar precio unitario DDP]</i>	<i>[indicar precio total DDP por cada artículo]</i>	<i>[Indicar el monto correspondiente a los impuestos]</i>	<i>[Indicar el porcentaje correspondiente a la alícuota del IVA]</i>
<b>Precio Total \$</b>							

Nombre del Licitante *[indicar el nombre completo del Licitante]* Firma del Licitante *[firma de la persona que firma la oferta]* Fecha *[Indicar Fecha]*

#### Anexo 4

#### MANIFIESTO DE GARANTIA DE LA OFERTA

*[El Licitante completará este Formulario de Manifiesto de Garantía de la Oferta de acuerdo con las instrucciones indicadas.]*

Fecha: *[indicar la fecha (día, mes y año) de presentación de la oferta]*  
LPN No.: *[indicar el número del proceso licitatorio]*

**A: Subsecretaría de Energías Renovables del Ministerio de Energía y Minería de La Nación.**

Nosotros, los suscritos, declaramos que:

1. Entendemos que, de acuerdo con sus condiciones, las ofertas deberán estar respaldadas por un Manifiesto de Garantía de la Oferta.
2. Aceptamos que automáticamente seremos declarados inelegibles para participar en cualquier licitación de contrato con el Comprador por un período de 2 años contado a partir de a partir de la apertura de la licitación si violamos nuestra(s) obligación(es) bajo las condiciones de la oferta si:
  - (a) retiráramos nuestra Oferta durante el período de vigencia de la oferta especificado por nosotros en el Formulario de Oferta; y/o
  - (b) no aceptáramos las correcciones aritméticas realizadas por el Comprador; y/o
  - (c) si después de haber sido notificados de la aceptación de nuestra Oferta durante el período de validez de la misma, (i) no ejecutamos o rehusamos ejecutar el formulario del Convenio de Contrato, si es requerido; o (ii) no suministramos o rehusamos suministrar la Garantía de Cumplimiento de conformidad con las instrucciones de la carta de invitación.
3. Entendemos que esta Manifiesto de Garantía de la Oferta expirará si no somos los seleccionados, y cuando ocurra el primero de los siguientes hechos: (i) si recibimos una copia de su comunicación con el nombre del Licitante seleccionado; o (ii) han transcurrido veintiocho días después de la expiración de nuestra Oferta.

Firmada: *[insertar la firma de la persona cuyo nombre y capacidad se indican].* En capacidad de *[indicar la capacidad jurídica de la persona que firma el Manifiesto de Garantía de la Oferta]*

Nombre: *[indicar el nombre completo de la persona que firma el Manifiesto de Garantía de la Oferta]*

Debidamente autorizado para firmar la oferta por y en nombre de: *[indicar el nombre completo del Licitante]*

Fecha el \_\_\_\_\_ día de \_\_\_\_\_ de 201\_\_\_\_\_ *[indicar la fecha de la firma]*

**Anexo 5**  
**LISTA DE BIENES Y PLAN DE ENTREGAS**

N° de Artículo	Descripción de los Bienes	Cantidad	Unidad física	Lugar de Entrega Final	Fecha de Entrega (de acuerdo a los <i>Incoterms</i> )	
					Fecha Límite de Entrega	Fecha de Entrega Ofrecida por el Licitante <sup>10</sup>
Ítem 1	Equipos datalogger para escuelas rurales	500	500	Av. Eduardo Madero 942 Piso 15-CABA	90 días desde la firma del contrato.	
Item 2	Desarrollo de software en soporte físico	1	1	Av. Eduardo Madero 942 Piso 15-CABA	90 días desde la firma del contrato	

<sup>10</sup> No se admiten plazos superiores a los máximos establecidos.

**Anexo 6**  
**AUTORIZACIÓN DEL FABRICANTE**  
**"NO APLICA"**

*[El Licitante solicitará al Fabricante que complete este formulario de acuerdo con las instrucciones indicadas. Esta carta de autorización deberá estar escrita en papel membrete del Fabricante y deberá estar firmado por la persona debidamente autorizada para firmar documentos que comprometan el Fabricante. El Licitante lo deberá incluir en su oferta, si así se establece en la Subcláusula 3.4.2 de la Sección B.]*

Fecha: *[indicar la fecha (día, mes y año) de presentación de la oferta]*  
LPN No.: *[indicar el número del proceso licitatorio]*

A: *[indicar el nombre completo del Comprador]*

**POR CUANTO**

Nosotros *[indicar nombre completo del Fabricante]*, como fabricantes oficiales de *[indique el nombre de los bienes fabricados]*, con fábricas ubicadas en *[indique la dirección completa de las fábricas]* mediante el presente instrumento autorizamos a *[indicar el nombre completo del Licitante]* a presentar una oferta con el solo propósito de suministrar los siguientes Bienes de fabricación nuestra *[nombre y breve descripción de los bienes]*, y a posteriormente negociar y firmar el Contrato.

Por este medio extendemos nuestro aval y plena garantía, conforme a la Subcláusula 4.1.2 de la Sección D, respecto a los bienes ofrecidos por la firma antes mencionada.

Firma: \_\_\_\_\_  
*[indicar firma del(los) representante(s) autorizado(s) del Fabricante]*

Nombre: *[indicar el nombre completo del representante autorizado del Fabricante]*

Cargo: *[indicar cargo]*

Debidamente autorizado para firmar esta Autorización en nombre de: *[nombre completo del Licitante]*

Fechado en el día \_\_\_\_\_ de \_\_\_\_\_ de \_\_ *[fecha de la firma]*

**Anexo 7**  
**FORMULARIO DE CONTRATO**

*[El Licitante seleccionado completará este formulario de acuerdo con las instrucciones indicadas]*

ESTE CONVENIO DE CONTRATO es celebrado

El día *[indicar: número]* de *[indicar: mes]* de *[indicar: año]*.

ENTRE

- (1) La Subsecretaría de Energías Renovables del Ministerio de Energía y Minería de La Nación , representada por el señor Subsecretario de Energías Renovables , Ingeniero Sebastián Alejandro KIND, D.N.I N° 27.333.333 y con domicilio legal en Avenida Paseo N° 189, Piso 9, oficina 903, de la Ciudad Autónoma de Buenos Aires, en adelante denominado “el Comprador”, y
- (2) *[indicar el nombre del Proveedor]*, una corporación incorporada bajo las leyes de *[indicar: nombre del país del Proveedor]* físicamente ubicada en *[indicar: dirección del Proveedor]* (en adelante denominada “el Proveedor”).

POR CUANTO el Comprador ha llamado a licitación respecto de ciertos Bienes y Servicios Conexos, *[inserte una breve descripción de los bienes y servicios]* y ha aceptado una oferta del Proveedor para el suministro de dichos Bienes y Servicios por la suma de *[indicar el Precio del Contrato en palabras y cifras expresado en la(s) moneda(s) del Contrato y]* (en adelante denominado “Precio del Contrato”), el cual se conforma de acuerdo al siguiente detalle:

Lote	Descripción	Cant.	Monto Total sin impuestos	Impuestos	Monto Total con impuestos DDP	Plazo de entrega

ESTE CONVENIO ATESTIGUA LO SIGUIENTE:

1. En este Convenio las palabras y expresiones tendrán el mismo significado que se les asigne en las respectivas condiciones del Contrato a que se refieran.
2. Los siguientes documentos constituyen el Contrato entre el Comprador y el Proveedor, y serán leídos e interpretados como parte integral del Contrato:
  - (a) Este Contrato;
  - (b) Las Condiciones Contractuales;
  - (c) La oferta del Proveedor y las Listas de Precios originales;
  - (d) Los Requerimientos Técnicos (incluyendo la Lista de Requisitos y las Especificaciones Técnicas);
  - (e) La notificación de Adjudicación del Contrato emitida por el Comprador.
  - (f) Planos *[en caso de corresponder]*
3. Este Contrato prevalecerá sobre todos los otros documentos contractuales. En caso de alguna discrepancia o inconsistencia entre los documentos del Contrato, los documentos prevalecerán en el orden enunciado anteriormente.

4. En consideración a los pagos que el Comprador hará al Proveedor conforme a lo estipulado en este Contrato, el Proveedor se compromete a proveer los Bienes y Servicios al Comprador y a subsanar los defectos de éstos de conformidad en todo respecto con las disposiciones del Contrato.
5. El Comprador se compromete a pagar al Proveedor como contrapartida del suministro de los bienes y servicios y la subsanación de sus defectos, el Precio del Contrato o las sumas que resulten pagaderas de conformidad con lo dispuesto en el Contrato en el plazo y en la forma prescritos en éste.

EN TESTIMONIO de lo cual las partes han ejecutado el presente Convenio de conformidad con las leyes de *[indicar el nombre de la ley del país que gobierna el Contrato]* en el día, mes y año antes indicados.

Por y en nombre del Comprador

Firmado: *[indicar firma]*  
en capacidad de *[indicar el título u otra designación apropiada]*  
en la presencia de *[indicar la identificación del testigo]*

Por y en nombre del Proveedor

Firmado: *[indicar la(s) firma(s) del (los) representante(s) autorizado(s) del Proveedor]*  
en capacidad de *[indicar el título u otra designación apropiada]*  
en la presencia de *[indicar la identificación del testigo]*

**Anexo 8  
GARANTÍA DE CONTRATO**

**Póliza de Seguro de Caucción**

PÓLIZA N° [indicar el número]

CONDICIONES PARTICULARES

Esta Compañía [indicar el **nombre de la Compañía Aseguradora**], EL ASEGURADOR, con domicilio en [indicar el **domicilio**], en su carácter de fiador solidario, con renuncia a los beneficios de excusión y división y con arreglo a las Condiciones Generales<sup>11</sup> que forman parte de esta póliza y a las Particulares que seguidamente se detallan, asegura a: [indicar el **Nombre del Comprador**], EL ASEGURADO, con domicilio en [indicar el **Domicilio del Comprador**] el pago de hasta la suma de [indicar **la moneda y el monto**] que resulte adeudarle [indicar el **nombre del Licitante**] EL TOMADOR, con domicilio en [indicar el **domicilio del Licitante**] por afectación de la garantía que de acuerdo a la ley, las bases de licitación y el contrato, en su caso, está obligado a constituir según el objeto que se indica en las Condiciones Generales integrantes de esta póliza.

OBJETO DE LA LICITACIÓN

Licitación [indicar **nombre y número del Llamado a Licitación**]

Contrato [indicar **nombre y número del Contrato**]

Préstamo/Crédito N°: [indicar: **número del préstamo o crédito**]

El presente seguro regirá desde la 0 hora del día [indicar **la fecha de la oferta**] hasta la extinción de las obligaciones del TOMADOR cuyo cumplimiento cubre.

Las cláusulas y anexos que seguidamente se detallan, firmadas y adheridas a las Condiciones Particulares, forman parte integrante de la presente póliza.

A los fines que hubiere lugar, EL ASEGURADOR, fija domicilio en: [indicar el **domicilio**]

Fecha: [indicar **fecha de emisión de la póliza**]

Por y en nombre de la Compañía Aseguradora:

\_\_\_\_\_  
(Firma)

\_\_\_\_\_  
(Firma)

\_\_\_\_\_  
(Nombre y cargo)

\_\_\_\_\_  
(Nombre y cargo)

Fecha: \_\_\_\_\_ en calidad de: [indicar: **cargo u otra designación apropiada**]

Sello de la Compañía Aseguradora

“Esta póliza ha sido aprobada por la Superintendencia de Seguros de la Nación (Resolución N°....).”

<sup>11</sup>Deberá adjuntarse la transcripción de las condiciones generales tipo aplicables a las pólizas de seguro de caucción.